HP StorageWorks Command Console V2.5

This guide provides information about installing, configuring, and operating Command Console software for the purpose of managing RAID array products.

hp ®

i n v e n t

Command Console V2.5 User Guide
Tenth Edition (March 2005)
Part Number: AA–RV1UA–TE

contents

Figures

Tables

This guide contains step-by-step installation instructions and serves as a reference for operation, troubleshooting, and future upgrades.

"About this Guide" topics include:

- "Overview", page 10
- "In This Guide", page 11
- "Conventions", page 12
- "Rack Stability", page 15
- "Getting Help", page 16

Overview

This section covers the following topics:

- Intended Audience
- Related Documentation

Intended Audience

- This guide is intended for storage administrators who have a basic understanding of storage and networks.

Related Documentation

In addition to this guide, HP provides corresponding information:

- Online help
- *HP StorageWorks Command Console V2.5 Release Notes*

In This Guide

This guide contains the following chapters and appendixes:

- Chapter 1—"About SWCC" provides a description of the function and capabilities of the SWCC application.

- Chapter 2—"Using SWCC" provides instructions on how to use SWCC.

- Chapter 3—"Setting Up Notification" provides instructions on how to set up notifications on SWCC.

- Chapter 4—"Interpreting Agent Email Messages" provides a description of how to interpret Agent email messages.

- Chapter 5—"Using the Storage Window" provides instructions on how to use Storage windows.

- Chapter 6—"Integrating SWCC with Insight Manager" provides instructions on how to integrate SWCC with the Insight Manager.

- Chapter 7—"Troubleshooting" provides instructions on how to troubleshoot SWCC.

- Appendix A—"Using the Command Console LUN" provides instructions on how to use the SWCC LUN.

- Appendix B—"Interpreting SNMP Traps" provides instructions on how to interpret SNMP trap messages.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document Conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

> **Tip:** Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

> **Note:** Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.
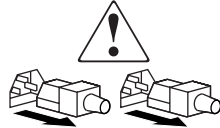
Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

> ⚠ **WARNING:** To reduce the risk of personal injury or damage to the equipment, be sure that:
> - The leveling jacks are extended to the floor.
> - The full weight of the rack rests on the leveling jacks.
> - In single rack installations, the stabilizing feet are attached to the rack.
> - In multiple rack installations, the racks are coupled.
> - Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

■   Technical support registration number (if applicable)

■   Product serial numbers

■   Product model names and numbers

■   Applicable error messages

■   Operating system type and revision level

■   Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access the storage web site at http://www.hp.com/country/us/eng/prodserv/storage.html and select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

■   In the United States, call 1-800-345-1518

■   In Canada, call 1-800-263-5868

■   Elsewhere, see the HP web site for locations and telephone numbers http://www.hp.com.

About SWCC

1

Product Overview

StorageWorks Command Console (SWCC) allows you to monitor and manage the storage connected to your HS-Series controller. Command Console is a management framework with a graphical user interface for managing HP StorageWorks RAID array products. SWCC runs on Microsoft Windows NT 4.0, Windows 2000, and Windows Server 2003 (32-bit). Refer to the SWCC Quickspecs for the latest service pack requirements. The SWCC Quickspecs are found at the web site. With SWCC, you can configure virtual disks, receive notification of events, and monitor your storage systems.

SWCC works with Client and Agent components. The Client program is designed for use on the Windows platform. It provides an easy method of configuring, operating, monitoring, and troubleshooting a particular subsystem. An Agent is a companion program that is installed on a host system running a supported operating system. The host system is connected to the controllers managed by SWCC. SWCC needs the Client and Agent to manage storage subsystems over a network.

Features

SWCC offers the following features:

- Manages HP StorageWorks RAID Arrays over a serial port, SCSI bus, or TCP/IP network.

- Configures RAID arrays using menus, icons, and system views.

- Provides the Navigation window and the ability to right-click to view properties.

- Configures arrays from files. Array configurations can be saved as files and used as a backup or to automatically configure other arrays.

- Monitors subsystems.

- Protects your access to subsystems and configuration with the password protection option.

- Interfaces with Windows NT, Windows 2000, or Windows Server 2003 logging capability on storage systems connected to Windows NT, Windows 2000, or Windows Server 2003 servers (not clients), and lists RAID array events in the NT event log.

- Notifies you of subsystem events via pager.

Components of SWCC

SWCC includes:

- Command Console—The Command Console consists of the Navigation tree, Navigation window, Asynchronous Event Service, and Pager notification.

- HS-Series Controller Client—The HS-Series Controller Client provides a Storage window that displays detailed information about a specific subsystem. From the Storage window, you can manage your subsystem, for example, by creating virtual disks.

- CLI Window—You can monitor and configure your subsystem by typing commands into the Command Line Interpreter (CLI) window. The CLI offers the same functionality as the Storage window. For more information, refer to the *HP StorageWorks HSG60 and HSG80 Array Controller and Array Controller Command Line Interface Reference Guide.*

- HS-Series Agent performs the following:
  - Obtains the status of the storage connected to the controller.
  - Passes the status of the devices connected to the controller to the Navigation tree, which passes the information to the Storage window.
  - Passes the status of the devices connected to the controller to the Event Viewer.
  - Provides email notification. This feature is not available on Windows 2000, Windows NT, or Windows Server 2003.

Refer to Table 2 for a summary of the SWCC features and required components.

Table 2: SWCC Features and Components

Features	Agent Required?	Client Required?
Ability to create storagesets	No	Yes
Ability to monitor many subsystems at once	Yes	Yes
Event logging	Yes	No
Email notification (Does not apply to Agents running on Windows NT 4.0, Windows 2000, or Windows Server 2003)	Yes	No
Pager notification	Yes	Yes

Client and Agent Versions

SWCC uses different clients and agents to provide storage management over a network. There is a single version of the Command Console that is used with all device-specific clients. There is a unique client for each supported HS-Series controller. There is an agent for each supported operating system though each agent is compatible with all supported controllers.

See the current versions of the Command Console, Agent, CLI window, and device-specific clients in Table 3.

Table 3: SWCC Component Versions

SWCC Component	Version
Command Console	V2.2.0
Agent	V2.5.0
SWCC CLI Window	V2.5.0
HSG80ACS85 Storage Window	V2.5.0
HSG80 Storage Window	V2.1.0
HSG60 Storage Window	V2.5.0

Command Console Client Minimum Hardware and Software Requirements

The minimum requirements to run the Command Console client properly are listed in Table 4.

Table 4: Minimum Hardware and Software Requirements

Item	Requirements
Management Station	Suggested minimum of a Pentium class system with 64 MB of RAM.
Operating System	Microsoft Windows NT 4.0 Windows 2000, and Windows Server 2003 (32-bit). Please refer to the SWCC Quickspecs for the latest service pack requirements.
Monitor	SVGA at 800x600 resolution, minimum*
Modem	Hayes-compatible (for event notification)
Serial Port	RS-232 (for local connection)
Network Adapter	TCP/IP-compatible network card (for distributed systems only)
Controller Compatibility	HSG80, HSG60
Host Software	ASPI SCSI driver required for host port virtual terminal connection (Windows NT only)

* Although it is possible to use the Client on a system with standard, VGA resolution, HP recommends that you use SVGA. The Storage window requires a minimum amount of screen space to properly display its contents. When you use VGA display resolution, screen space becomes more limited. For more information, see "Storage Window Display", page 67

Network Specifications

SWCC is a terabyte-class RAID Array manager. Fully scalable, SWCC can manage a single, locally connected RAID array or RAID arrays in a multi-node, TCP/IP network environment. SWCC can support a number of Clients and Agents in a distributed environment.

Connections Supported by SWCC

SWCC manages storage by using Storage windows. Storage windows are device-specific clients that communicate with storage devices either directly or through an agent. Storage windows are used to configure and monitor storage arrays. An agent is connected to storage controllers, which the agent configures and monitors.

There are several different types of connections used by the clients to communicate with storage controllers and agents.

SWCC provides storage management over the following connections, as listed in Table 5:

■ Direct Serial connection

■ SCSI connection

■ Storage Area Network (SAN) and TCP/IP network

Table 5: SWCC Connections for HS-Series Controllers

Connection	Agent Required?
SAN and TCP/IP network connection	Yes
Direct serial connection	No*
SCSI connection**	No**

* If you do not install Agent, you cannot use the Navigation tree or Pager notification.
** SCSI over Fibre Channel is available with HSG60 and HSG80 controllers.

Note: SWCC does not support the Dynamic Host Configuration Protocol (DHCP) or the Windows Internet Name Service (WINS).

To determine whether your system is using DHCP or WINS on Windows NT 4.0:

1. Right-click **Network Neighborhood** on the desktop.

2. Select **Properties**.

3. Click the **Protocols** tab.

4. Select **TCP/IP**, and then click **Properties**. The Microsoft TCP/IP Properties window opens.

To determine whether your system is using DHCP or WINS on Windows 2000 or Windows 2003:

1. Right-click **My Network Place**s on your desktop.

2. Select **Properties**.

3. In the **Network and Dial-up Connections** window which opens, right-click the connection to be used by SWCC.

4. Select **Properties**.

5. Select **Internet Protocol (TCP/IP)**, then click **Properties**.

The Microsoft TCP/IP Properties window opens.

SAN and TCP/IP Network Connection

By using a network connection, as shown in Figure 1, you can configure and monitor your storage subsystem from anywhere on your Local Area Network (LAN). If you have a Wide Area Network (WAN) or a connection to the Internet, you can monitor your subsystem with TCP/IP.

SWCC can include a number of Clients and Agents in a network. However, it is suggested that you install only one HS-Series Agent on the computer that has a connection to the HS-Series controller.
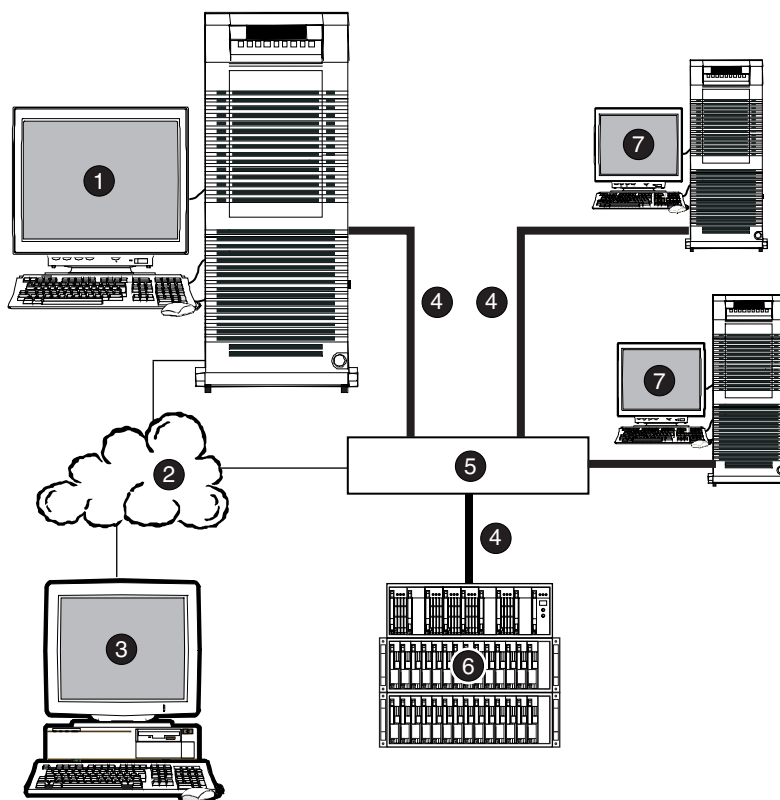
CXO7240A

❶	Agent system (has Agent software)	❸	Client system (has Client software)	❻	Storage system
❷	TCP/IP network	❹	Fibre Channel cable	❼	Servers
		❺	Hub or switch		

Figure 1: SAN and TCP/IP network connection

Local Serial Port Connection

A local serial port connection uses only the Storage window to manage your storage subsystems. The client system is connected to the subsystem by a serial connection, as shown in Figure 2.

Note: Local serial connections are available only with standalone Storage windows. You cannot use the Command Console Navigation window to connect locally to a subsystem.

SHR-1598B
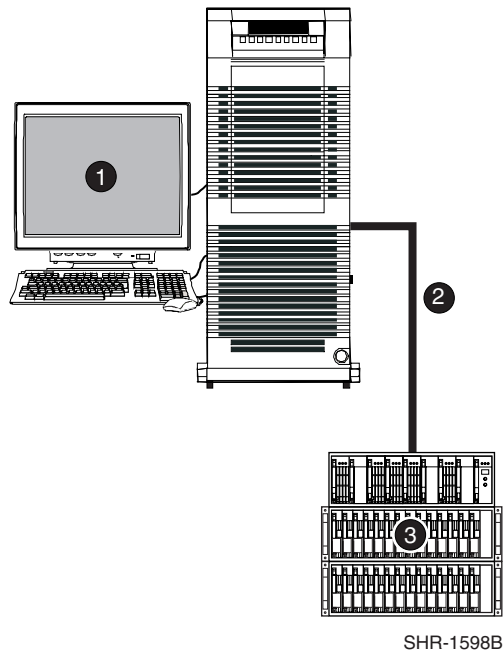
❶ Client system
❷ Serial connection
❸ Storage system

Figure 2: Local serial port connection

SCSI Connection

A SCSI connection over a SCSI bus or using the Fibre Channel bus, as shown in Figure 3, uses only the Storage window to manage your storage system. The HSG60 and HSG80 controllers support the SCSI over Fibre Channel bus connection.

Note: Local SCSI connections are available only with standalone Storage windows. You cannot use the Command Console Navigation window to connect locally to a subsystem.
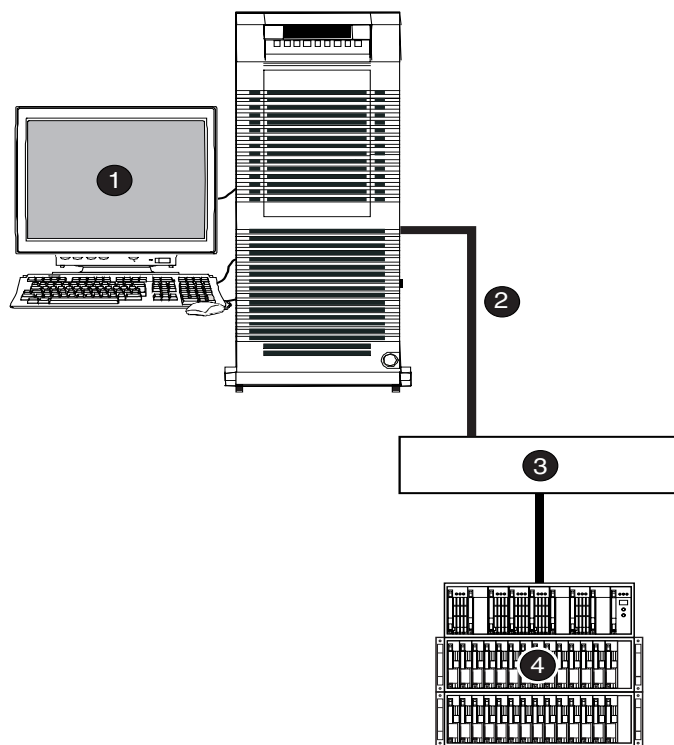
SHR-1597B

❶   Client system that has the Storage window
❷   Fibre Channel cable (using SCSI connection)
❸   Hub or switch
❹   Storage system

Figure 3: SCSI connection using Fibre Channel cable

Accessing the Storage Window

You can access the HS-Series Storage window from the Start menu. You can connect the Storage window to storage over a serial connection, a SCSI connection, or a TCP/IP network.

Before you can make either a SCSI or a network connection, you must have one of the following:

■   A virtual disk created on the subsystem

■   Command Console LUN (CCL) enabled

For more information about:

■   Creating a virtual disk, see the section titled "Creating Virtual Disks", page 72

■   Enabling and disabling the CCL, see Appendix A,

■   Accessing the Storage window from the Navigation tree, see the section titled "Managing Storage Subsystems from the Navigation Tree", page 40

Serial Connections

The simplest connection to a subsystem is a direct cable connection from the Client's host system to a serial port on the subsystem. The serial connection is often used to set the initial configuration of a storage subsystem. This initial configuration can then allow a SCSI or network connection to the subsystem.

A direct serial connection to a subsystem does not provide as much functionality as a network connection. The agent is bypassed so that any agent-related function is not available. These functions include event logging, email, and pager notification. The Navigation tree is not available with a direct serial connection.

To set up a serial connection:

1.   Click **Start > Programs > Command Console > StorageWorks CC HSxxx**. The Connection Selection window opens, as shown in Figure 4.
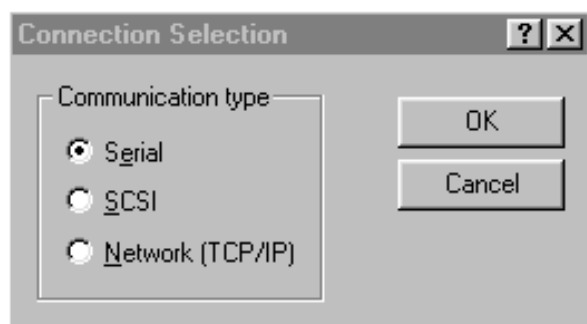
Figure 4: Connection Selection dialog box

2. When the Connection Selection window opens, choose **Serial** and then click **OK**. The Connect Serial window opens, as shown in Figure 5.

3. From the drop-down menu, choose the COM port connected to the RAID HS-Series controller.

4. Choose a controller baud rate, a Subsystem Physical View, or a Subsystem Grid View. Click **Connect.** When the Storage window opens, you are connected to your subsystem.
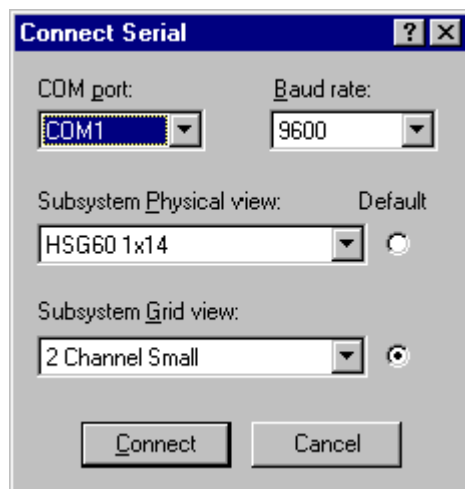
Figure 5: Connect Serial window

SCSI Connections

The SCSI connection uses the SCSI bus or Fibre Channel bus that is the primary data channel for the storage subsystem. The amount of management information that passes between the Storage window and the subsystem is small compared to the amount of data moved by a typical storage request.

Like the direct serial connection, the SCSI connection does not use an agent. The SCSI connection only supports a Storage window or CLI window without a Navigation tree. There is no event logging, email, or pager notification with a SCSI connection.

Establishing a SCSI connection requires that a Command Console LUN or a virtual disk be configured on the storage subsystem.

1. Click **Start > Programs > Command Console > StorageWorks CC HSxxx**.

2. When the **Connection Selection** dialog box displays, select the **SCSI** option. The **SCSI Setup** window opens, as shown in Figure 6.

3. Select a drive mapped to the subsystem or a CCL, and then click **Connect**.

   Command Console connects to the storage subsystem and displays the corresponding Storage window.
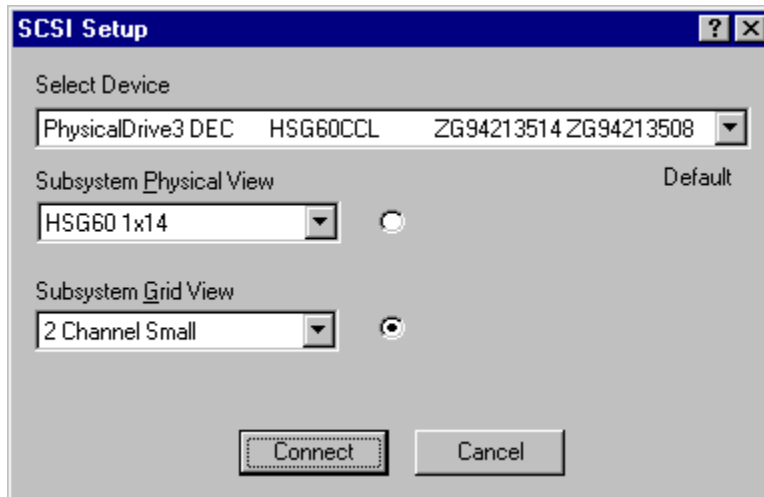
Figure 6: SCSI Setup window

Network Connections

Using SWCC with a network connection provides you with more features and flexibility for managing storage subsystems than serial or SCSI connections. A network connection between a client and agent supports the use of the Navigation tree, allowing for the management of multiple subsystems from a single application. The use of an agent enables event logging on the agent host and also email and pager notification for subsystem events.

A network connection requires that an agent be installed on a host connected to the storage subsystem. Establishing a network connection requires that a Command Console LUN or a virtual disk be configured on the storage subsystem. If the storage subsystem is not properly preconfigured, then a serial connection must be used to enable the Command Console LUN or to create a virtual disk.

To use SWCC to manage the HS-Series controller over a network, install the Command Console, the HS-Series device-specific Client (Storage window), and the HS-Series Agent. The Command Console and the HS-Series Client are installed together.

To set up SWCC to manage the HS-Series controller over a network:

1. Click **Start > Programs > Command Console > StorageWorks CC HSxxx**. The Client displays the **Connection Selection** window.

2. Choose the **Network (TCP/IP)**.

   The **Connect Network (TCP/IP)** window opens, as shown in Figure 7.
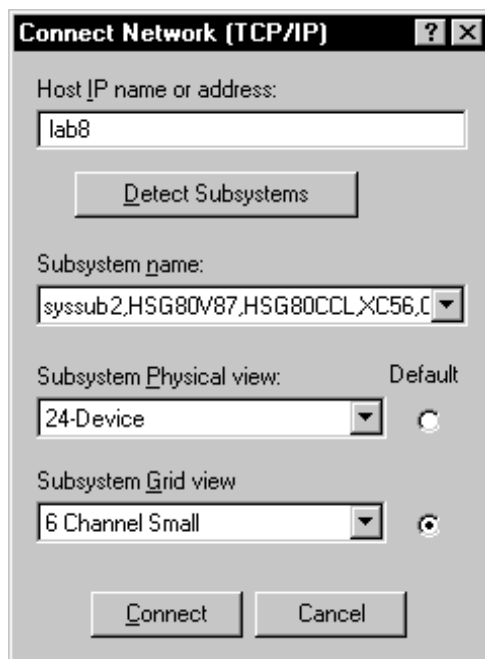
Figure 7: Connect Network (TCP/IP) window

3. Enter the host IP name or address in the text box, and then click **Detect Subsystems**.

   The Client locates the subsystem connected to the host.

4. Choose the subsystem, and then click **Connect**.

   The Client displays the Storage window.

The controller maintains a table of host port connections that can contain up to 96 named connections. However only 8 of those connections can be active at any time. The Client shows only those connections that the controller recognizes as online.

Connection Features and Limitations

Because of the nature of the connections you can use between the Client and your subsystems, the features available with each connection type vary slightly. Some connection types impose limitations on the Client's features, as noted in Table 6.

Table 6: Feature Limitations

Feature Connection Type	Create Virtual Disk	Delete Virtual Disk	Fault Events: Client Visual Notify	Fault Events: Paging Notify	Windows NT/ 2000/ Server 2003 Fault Events: Event Logging	Email Notify (UNIX/V MS only)
Local Serial Connect (Storage Window Manager and Agent not used)	Supported	Supported	Supported	Not Supported	Not Supported	Not Supported
Local SCSI Bus Connect (Storage Window Manager and Agent not used)	Supported	Supported	Supported	Not Supported	Not Supported	Not Supported
Local Network Connect (Client and Agent running on the same host)	Supported	Supported	Supported	Supported	Supported	Not Supported
Remote Network Connect (Client running on a PC remote from Agent on a host)	Supported	Supported	Supported	Supported	Supported	Supported

Table 6: Feature Limitations (Continued)

Feature Connection Type	Create Virtual Disk	Delete Virtual Disk	Fault Events: Client Visual Notify	Fault Events: Paging Notify	Windows NT/ 2000/ Server 2003 Fault Events: Event Logging	Email Notify (UNIX/V MS only)
RAS Connect (Client running on a remote PC with a dialup network connection)	Supported but not recom-mended. Follow-up operating system configura-tion cannot be performed remotely.	Supported but not recom-mended. Follow-up operating system configura-tion cannot be performed remotely.	Supported reliably only while RAS intact. Some events may be missed while dialup connec-tion is broken.	Supported reliably only while RAS intact. Some events may be missed while dialup connec-tion is broken.	Supported reliably at host end only. Some events may be missed at Client end while dialup connec-tion is broken.	Supported

Local Client/Agent Network Connection

You can run both the Client and Agent on the same Windows NT, Windows 2000, or Windows Server 2003 host machine and connect them using a network connection. By doing so, you can create a local connection to take advantage of the Agent's event notification features. No special installation instructions are necessary to implement this type of connection. Install each component as if the Client were to run on a system remote from the host machine.

Because the Client runs only on Windows NT, Windows 2000, and Windows Server 2003 systems, and the Agent runs on Windows NT, UNIX-based systems, and OpenVMS, you can implement this type of connection only on a Windows NT system. Also, you cannot use a Client with a local connection of either type while an Agent is running on the local machine.

Note: SWCC is no longer supported on Novell NetWare systems with HBA 281540-B21 (3R-A3750-AA).

Using Command Console

2

Using the Navigation Tree

The Navigation tree is displayed in the Navigation window. The Navigation tree lets you view the status of all your storage at once, as shown in Figure 8. Note that some items shown in this Navigation tree may not represent the software in your release.
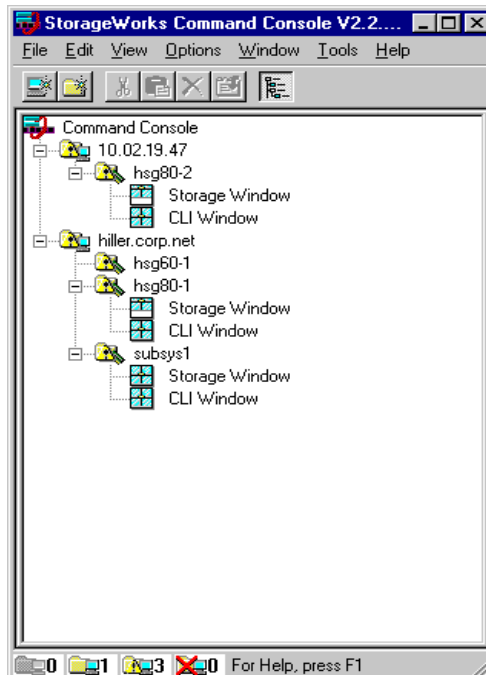
Figure 8: An example of the Navigation tree

Adding a Storage Subsystem to the Navigation Tree

The Navigation tree allows you to manage your storage over the network from the Storage window. If you plan to use pager notification, you must add the storage subsystem to the Navigation tree.

To add the storage subsystem to the Navigation tree:

1. Verify that you have properly installed and configured the HS-Series Agent on the storage subsystem host. For more information, refer to the installation and configuration guide for your operating system.

2. To display the Navigation window, click **Start > Programs > Command Console > StorageWorks Command Console**.

3. Click **File > Add System**.

    The **Add System** window opens.

4. Type the host name or its TCP/IP address and click **Apply**.

5. Click **Close**.

6. Click the **plus sign (+)** to expand the host icon.

7. To access the Storage window for the subsystem, double-click the Storage window icon.

Managing Storage Subsystems from the Navigation Tree

You can manage a storage subsystem from the Navigation tree by double-clicking the Storage window or CLI window icon.

To access a subsystem window:

1. Double-click the folder for the storage subsystem.

    Up to two icons may be displayed underneath the folder. This depends on whether you have installed the Storage window and the CLI window.

2. Double-click the Storage window or CLI window icon for the subsystem.

Organizing Your Storage in the Navigation Tree

After you add systems to the Navigation tree, you can organize your storage in folders:

■   You can place folders under the Command Console root or under another general folder in the Navigation window.

■ You can use folders to group systems and other general folders. Note that you cannot use folders to group controllers.
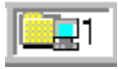
For example, in Figure 8, the general folder *Storage on the First floor* was created and two agent systems were placed in the folder. If a system in the folder is at a critical state, the status of the folder displays the same critical state.

Note: For a description of the Command Console Navigation tree, refer to the "Quick Tour" in the introduction of the Command Console Client online Help.

About the Navigation Tree Icons

The Navigation tree icons listed in Table 7 change to show system status. The Navigation window status bar, located in the lower-left corner, summarizes the host system connection status.

Table 7: Description of Icons in Navigation Window Status Bar

Icon	Description
	Indicates the number of disconnected systems
	Indicates the number of fully functional systems
	Indicates the number of degraded systems
	Indicates a critically failed system

About the Asynchronous Event Service

The Asynchronous Event Service (AES) does the following:

■ Runs in the background as a service that provides status updates of the subsystems to its client system. A client system must run AES to receive updates.

■ Passes the trap (message) to the Navigation tree. The Navigation tree, in turn, passes the trap to the appropriate Storage window. When a trap provides information about a status change in a subsystem, one or more of the icons in the Navigation tree change color or the symbol changes.

■ Send traps to pagers. To activate this feature, you must predefine each pager number in the User Profile section of the Event Notification menu in the Navigation window.

Note: Refer to Command Console's online Help for the latest information about how to diagnose problems that can occur when sending pages. Help provides instructions on how to put AES into a debug mode.

AES Functionality

You can modify how AES starts. You can also manually stop or start AES. However, you must run AES to receive pager notification of events and to provide updates to the Navigation tree, Storage windows, and Event Viewer. If you stop AES, the Client software stops the following functionality:

■ Updates to the Navigation tree and Storage windows

■ Updates from AES in the application log of the Event Viewer

■ Notifying pagers if a fault occurs

To Stop or Start AES

From Windows NT

To stop or start AES manually:

1. Double-click **Services** in Control Panel.

2. Click the **AsyncEventSvc** entry.

3. Click **Stop or Start**, and then click **Close**.

To disable AES from starting automatically when your system boots, change the startup option to manual in the Services window. Use the following steps:

1. Double-click **Services** in Control Panel.

2. Double-click the **AsyncEventSvc** entry.

    The **Services** window opens.

3. Choose **Manual** under **Startup Type**, and click **OK**.

From Windows 2000 and Windows Server 2003

To stop or start AES manually:

1. Click **Start > Settings > Control Panel > Administrative Tools > Component Services**.

2. Under **Console Root**, choose **Services (Local)**.

3. Under **Services (Local)**, right click **AsyncEventSvc**.

4. Click **Stop or Start**.

To disable the automatic start of AES, at system boot, change the startup option to manual:

1. Click **Start > Settings > Control Panel > Administrative Tools > Component Services**.

2. Under **Console Root**, choose **Services (Local)**.

3. Under **Services (Local)**, right click **AsyncEventSvc**.

4. From the drop-down menu, choose **Properties**.

    The **AsyncEventSvc Properties (Local Computer)** window opens.

5. Under the **General** tab, choose **Manual** from the **Startup Type** drop-down menu.

6. Click **OK**.

Setting Up Notification

3

Required Components for Notification

Table 8 lists the notification options available with SWCC and the components required for each option.

Table 8: Required Components for Notification

Notification Option	Required Components
Navigation tree	Client and Agent
Pager	Client and Agent
Email notification (applies to certain agents)	Agent
Event logging	Agent
SWCC with third-party storage management program	Agent and third-party storage management program

Setting Up Pager Notification

You can set up Command Console to notify you by pager when a critical event occurs. This feature works with alphanumeric and numeric pagers. You can configure paging to notify multiple pagers for multiple storage subsystems within different blocks of time. For example, if several people monitor your network in shifts, you can configure paging so the software pages only those people working the current shift. You can also temporarily disable any pager.

To receive pages, the following must occur:

■ The AES must be running on the client system on which you set up the pager notification.

■ The Agent must be running.

■ The client system must be added to the Agent's list of client system entries.

■ In the Agent's list of client system entries, you must select the TCP/IP notification scheme for your client system.

■ You must add the Agent system to the Navigation tree of the client system on which you set up pager notification.

Note: Pager notification uses the Telocator Alphanumeric Protocol (TAP) adopted in 1988 by the Personal Communications Industry Association (PCIA). Verify that your paging company uses this protocol.

Table 9 lists and describes the steps to use to set up pager notification.

Table 9: Setting Up Pager Notification

Step	Description	Refer to Section
1	Numeric Pagers only - assign pager codes to host systems and controllers.	Setting Up Pager Codes.
2	Set up user profiles.	Setting Up User Profiles.
3	Set up notification lists.	Setting Up Notification Lists.
4	Set up modem and polling intervals.	Setting Up Modem and Polling Preferences.
5	Associate systems and controllers with notification list.	Associating My Enterprise, Systems, and Subsystems with Notification Lists.

Setting Up Pager Codes

Numeric pager support lets you receive notification about critical events.

A numeric pager usually has three fields separated by hyphens. The first field signifies the area code, the second field signifies the exchange, and the third field signifies the four-digit extension.

A page from Command Console is structured as follows:

■ First field is a three-digit number for the host system.

■ Second field is a three-digit number for the subsystem.

■ Last field is a four-digit code for the critical event.

To set up pager codes, first assign a three-digit code for each host system, and then assign another three-digit code for each subsystem controller connected to that host. The last four digits are pre-assigned.

To Assign a Pager Code to a Host System:

1. Click a host system in the Navigation window.

2. Click **File > Properties.**

3. Click the **Event Notification** tab.

4. Enter a three-digit number in **Pager identification number**. Avoid entering a number that may be mistaken for an area code.

To Assign a Pager Code to a Subsystem:

1. Click a subsystem controller in the **Navigation** window.

2. Click **File > Properties.**

3. Click the **Event Notification** tab.

4. Enter a three-digit number in **Pager identification number**.

To View or Change a Pager Code for a Critical Event:

1. Click **Options > Event Notification > Pager Codes.**

2. Click the code you want to edit, and then click **Edit**.

3. Type the new pager code in the **Edit** field.

The default pager codes are listed in Table 10.

Table 10: Default Pager Codes

Critical Event	Code	Notes
Disk Fault	1000	Physical device failure
Power Supply Fault	1002	
Fan Fault	1003	
Battery Fault	1004	
Temperature Fault	1005	
Controller Fault	1006	The controller detected an internal fault
Communication Fault	1007	Agent cannot talk to the subsystem.
Other controller fault	1008	One controller is reporting a fault on the other.
External fault	1009	
LUN Fault	1010	Virtual disk failure

Note: All codes are numeric-only; alphanumeric pager codes are not supported.

Setting Up User Profiles

1. Click **Options > Event Notification > User Profiles**.
2. Click **New**.
3. Type a name. You can also enter a description.
4. Click the **Pager** tab.
5. Choose **Enabled** to enable paging to this person.
6. Enter the phone number for your pager in the **Pager Number** field, along with any prefixes required to reach the outside phone system.

   Optionally, you can use one or more commas to specify a wait intervals for numeric pager numbers. Each comma causes the pager dialer to wait two seconds before sending the PIN to the paging company. An example is: 8,,1, 800,5551212. In this example, there is a 4-second delay between the 8 and the 1.

7. Check **Alphanumeric** if the paging system supports alphanumeric paging. Leaving the box blank results in numeric paging only.

8. Type the pager identification number (PIN). (This is required for alphanumeric pagers). If your numeric pager does not require a PIN, leave the field blank. For example, this field must be blank for numeric pagers that are assigned a unique telephone number.

9. Type the start and end times that this person is available for paging, in the format HH:MM using a 24-hour clock. If you want 24 hour coverage, enter a start time of 00:00 and an end time of 24:00. You must enter a time period for paging. If you leave the start and end times at 00:00, paging is cancelled for this person.

10. Click **OK** to close the **Edit Profile** dialog box.

Keep the following in mind:

■   If you dial a code to access an outside number, the code must precede the phone number in the pager number field.

■   Do not use commas with alphanumeric pagers, except to access an outside line.

■   You may need to add more commas to make the Command Console pause long enough for the pager company greeting to complete.

■   Alphanumeric pagers require you to supply the paging service provider's TAP service modem number in the pager number field.

■   Not every paging company requires a PIN. If your pager is assigned a unique phone number for calling the paging company, do not enter a PIN.

■   Alphanumeric pagers require a PIN.

■   Refer to your pager documentation to determine which special characters are supported.

Figure 9 shows a sample user profile for an alphanumeric pager, and Figure 10 shows a sample user profile for a numeric pager.

Figure 9: Sample user profile – alphanumeric paging

Figure 10: Sample user profile – numeric paging

Note: The commas in the Identification Number field represent two-second wait intervals.

Setting Up Notification Lists

Use notification lists to notify groups about critical events. Be sure to first create a user profile for each user in the group. You cannot add users to the notification list unless they have user profiles. Then, use the Properties pages to associate notification lists with system and subsystem critical events.

1. Click **Options > Event Notification > Notification List**.
2. Click **New** and enter a name for the new notification list.
3. Write a brief description of the list (optional).
4. Add members to the list by clicking the check box next to each name.

Setting Up Modem and Polling Preferences

The subsystem polling interval is the frequency at which the Client pings an Agent to determine if it is running.

1. Click **Options > Preferences**.

2. Type the number of hours or minutes in the subsystem polling interval field. The default-polling interval is 30 minutes.

3. Select the COM port in your computer that your modem uses.

4. For alphanumeric pagers, select the baud rate (typically, it is 1200) of your paging service provider's TAP modem.

Associating My Enterprise, Systems, and Subsystems with Notification Lists

You can associate host systems and subsystems with notification lists for the purpose of paging a group if a critical event occurs. You can establish paging on three separate levels:

■   My Enterprise

■   System Level

■   Subsystem Level

You can configure paging on all levels or any combination of levels.

Before you can associate a system or controller with a notification list, you must first create a notification list. See "Setting Up Notification Lists", page 51.

My Enterprise

Use My Enterprise to notify all notifications lists listed here for problems on all systems and subsystems.

1. Highlight **My Enterprise** in the Storage Window Manager and then choose **File > Properties > Event Notification** from the menu.

2. Click the **Notification List** box to show all of the lists you have created.

3. Choose the list of persons who should be notified in case of a failure on any system.

System Level

Use the System Level to notify all notifications lists about problems on the specific system and its selected subsystems.

1. Highlight the desired system name in the Storage Window Manager and then choose **Start > Programs > File > Properties > Event Notification**.

2. Click the **Notification List** box to show all of the lists you have created.

3. Choose the list of persons, who should be notified in case of a failure on any subsystem of this specific system.

Subsystem Level

Use the Subsystem Level to notify all notifications lists listed here for problems on the selected subsystem.

1. Highlight the desired system name in the Storage Window Manager and then choose **Start > Programs > File > Properties > Event Notification**.

2. Click the **Notification List** box to show all of the lists you have created.

3. Choose the list for persons who should be notified in case of a failure on this specific subsystem.

Using SWCC with a Third-Party Storage Management Program

To use SWCC with a third-party storage management program:

1. Add the name of the computer on which the third-party storage management program resides to the Agent's list of client system entries. Select SNMP as the notification scheme. The Agent sends SNMP traps to every client system on its list.

    For more information on how to add client systems, see the Installation and Configuration Guide for your Agent.

2. Use the compiler that came with your third-party storage management program to compile the Management Information Base (MIB) file, `hs-agent.mib` in this kit.

Note: Depending on the third-party software, you may need to perform additional steps. Refer to the third-party storage management program documentation.

Using Event Logging on the Client System to Monitor Your Subsystem

The Agent can place SNMP and TCP/IP traps in the Application Log of Event Viewer, which is a part of Windows NT, Windows 2000, and Windows Server 2003. The HS-Series Agent collects events from the controllers and lists the events under the source, AsyncEventSvc. If the Agent is installed on Windows NT, Windows 2000, and Windows Server 2003, you can locate its entries in the Application Log by looking for `steam` under the Source column.

For a client system to receive event logs from an HS-Series Agent on another computer:

■ The client system must appear on the Agent's list of client system entries and TCP/IP must be selected as a notification scheme.

■ The AES must be running on the client system.

■ The Agent must be running.

To access Event Viewer:

■ Windows NT 4.0—Click **Start > Programs > Administrative Tools > Event Viewer** to access the Application Log. Choose **Application** from the Log menu.

■ Windows 2000 and Windows Server 2003—Click **Start > Settings > Control Panel > Administrative Tools > Event Viewer** to access the Application Log. Choose **Application Log** in the tree panel.

For more information about SNMP traps, see Chapter 5.

Interpreting Agent Email Messages

4

> **Note:** This chapter does not apply to the HS-Series Agents running on Windows NT 4.0, Windows 2000, or Windows Server 2003.

Most of the information in this chapter pertains to the event information email messages that the RAID Manager agent sends when an event occurs. If the Agent email notification feature is enabled when a RAID system event occurs, the Agent sends notification to the specified email addresses. A storage system event can be a change in the state of a physical storage device, a logical storage unit, or a component of the physical enclosure.

The message specifies the name of the host to which the RAID array reporting the event is connected. The message states the severity of the problem as one of these three levels:

■ Critical

■ Warning

■ Informational

The email message is displayed in the following format:

```
        ----------------
From RaidManager Tue Oct 6 15:59:59 1998
Date: Tue, 6 Oct 1998 15:59:58 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!
Hostname: Suncity
CRITICAL: Validation failed - Unauthorized client
(shr-dhcp-24-188.shr.dec.com, access level: -1); connection
refused (SP_TCP: ClientConnect)

End Of Automatic Message.
-------------------
```

About Event Information Fields

Event information messages report on the state of the RAID system. The event information fields appear in the line following the problem severity level.

Example:

```
WARNING:-
Suncity HSG80 12000000000 HSG80 disks(disk21100:2) (SP_MONITOR:
MonitorSubsys)
        \       \          \
         \       \          \
        (1)    (2)      (3)
```

Use the following information to help you to understand event information fields:

■ Host Name—The name of the host to which the RAID experiencing the event is connected.

■ Storage System—Where the problem occurred.

■ State Change—The specified component of the storage system. This is an 11-digit field that provides important information about the status of your RAID Array.

Mapping State Change Digits to RAID System Components

Each of the 11 digits in the state change field can be mapped to a RAID system component. Table 11 lists the digits and their relationship.

Table 11: State Change Digit Position and Corresponding RAID System Component

State Change Digit Position	Corresponding RAID System Component
1	Overall RAID System
2	Disks
3	Power Supply
4	Fans
5	Battery
6	Temperature
7	This Controller
8	Communications LUN
9	Other Controllers
10	External Factors
11	Logical Units

The First Digit of the State Change Field (Overall RAID System)

The first digit in the state change field reports state changes in the overall RAID system.

Example:

```
WARNING: -
Suncity HSG80 12000000000 HSG80 disks(disk21100:2)(SP_MONITOR:
MonitorSubsys)
```

The first digit can have one of two values:

0—Everything is fine.
1—Something has changed state.

The Second Digit of the State Change Field (Disks)

The second digit of the state change field reports state changes in disks.

Example:

```
WARNING: -
Suncity HSG80 12000000000 HSG80 disks(disk21100:2)(SP_MONITOR:
MonitorSubsys)
```

This digit can have one of three values:

0—Everything is fine.
1—Drive went from bad to good.
2—Drive went from good to bad.

In this example, a value of 2 is displayed in the disk digit position, indicating that a drive went from good to bad.

The disk name (in parentheses) follows, in the format:

```
disk_name:state
```

where *disk_name* is the name of the disk and *state* can be either of the following:

1—Disk went from bad to good.
2—Disk went from good to bad.

In this example, the failed drive is disk21100.

The Third Digit of the State Change Field (Power Supply)

The third digit of the state change field reports state changes in the power supply.

Example:

```
WARNING: -
Suncity HSG80 10200000000 HSG80 pwr(0:1:2) (SP_MONITOR:
MonitorSubsys)
```

The third digit can have one of three values:

0—Everything is fine.
1— Power supply went from bad to good.
2—Power supply went from good to bad.

The position (in parentheses) of the failed power supply usually follows. Three numbers indicate the position in the format:

```
cabinet_number:power_position:state
```

where *cabinet_number* is the cabinet ID from 0 to 1, the *power-position* is the power supply location (1 or 2), and *state* is one of the following:

1—Power supply went from bad to good.
2—Power supply went from good to bad.
3—Power supply is not present.

In this example, the power supply in position 1 of cabinet 0 (main cabinet) went from good to bad.

The Fourth Digit of the State Change Field (Fans)

The fourth digit of the state change field reports state changes in fans.

Example:

```
WARNING: -
Suncity HSG80 100200000000 HSG80 fans(0:A:2) (SP_MONITOR:
MonitorSubsys)
```

The fourth digit can have one of three values:

0—Everything is fine.
1—Fan state went from bad to good.
2—Fan state went from good to bad.

The position (in parentheses) of the fan follows, in the format:

```
cabinet_number:fan_position:state
```

where *cabinet_number* is the cabinet ID from 0 to 1, *fan_position* is the position of the fan, and *state* is either of the following:

1—Fan went from bad to good.
2—Fan went from good to bad.

In this example, a fan failure occurred in cabinet 0, the main cabinet.

The Fifth Digit of the State Change Field (Battery)

The fifth digit reports battery state change.

Example:

```
WARNING: -
Suncity HSG80 10002000000 HSG80 batt(6:fail) (SP_MONITOR:
MonitorSubsys)
```

The fifth digit can have one of three values:

0—Everything is fine.
1—Battery state went from bad to good.
2—Battery state went from good to bad.

The details of the battery failure follow in parentheses, in the format:

```
controller_id:state
```

where *controller_id* is the SCSI ID of the reporting controller (in other words, the cache battery failed for the other controller), and *state* is one of the following:

Good—Battery is good.
Low—Battery voltage is low.
Fail—Battery has failed.

In this example, the cache battery for the controller with SCSI ID 6 failed.

The Sixth Digit of the State Change Field (Temperature)

The sixth digit of the state change field reports temperature state changes.

Example:

```
WARNING: -
Suncity HSG80 100002 00000 HSG80 temp(0:2:2) (SP_MONITOR:
Monitor_Subsys)
```

The sixth digit can have one of three values:

0—Everything is fine.
1—Temperature state went from bad to good.
2—Temperature state went from good to bad.

The details regarding the temperature change follow in parentheses, in the format:

```
cabinet_number:sensor_type:state
```

where *cabinet_number* is the cabinet ID from 0-1, *sensor_type* is the EMU sensor (sensor 1 or sensor 2), and *state* is either of the following:

1—Temperature went from bad to good.
2—Temperature went from good to bad.

In this example, an adverse temperature change is detected by sensor 2 of the main cabinet.

The Seventh Digit of the State Change Field (This_Controller)

The seventh digit reports state changes in This_Controller.

Note: This value is always 0 for a dual redundant configuration.

Example:

```
Suncity HSG80 10000002000 HSG80 (SP_MONITOR: MonitorSubsys)
```

This digit can have one of two values:

0—Everything is fine.
1—Failure of the controller in a single-controller configuration.

The Eighth Digit of the State Change Field (Communications LUN)

The eighth digit reports the state changes in the communications LUN.

Example:

```
CRITICAL: - Suncity HSG80 10000002000 HSG80 (SP_MONITOR:
MonitorSubsys)

CRITICAL: Unable to open device - hdisk1 (SP_MONITOR:
MonitorSubsys)
```

This digit can have one of three values:

0—Everything is fine.
1—Communications LUN is available to the host machine.
2—Communications LUN is not available to the host machine.

In this example, two email messages appear. The first message indicates that a communications LUN changed state from good to bad. The second message indicates that the Agent is unable to open the communications LUN for monitoring the RAID system.

The Ninth Digit of the State Change Field (Other_Controller)

The ninth digit reports states changes in the Other_Controller.

Example:

```
WARNING: -
Suncity HSG80 10000000200 HSG80 (SP_MONITOR: MonitorSubsys)
```

This value never changes for a single controller configuration. It always changes if either controller in a dual redundant configuration fails.

This digit can have one of three values:

0—Everything is fine.
1—Both controllers are functioning.
2—One of the two controllers failed.

Physically inspect the controllers to verify which one failed, as indicated by a solid green indicator light (not blinking).

The 10th Digit of the State Change Field (External Factors)

The 10th digit indicates state changes caused by external factors.

Example:

```
WARNING: -
Suncity HSG80 10000000020 HSG80 (SP_MONITOR: MonitorSubsys)
```

This digit can have one of three values:

0—Everything is fine.
1—State changed from bad to good.
2—State changed from good to bad.

The 11th Digit of the State Change Field (Logical Units)

The 11th digit reports state changes in logical units.

Example:

```
WARNING: -
Suncity HSG80 10000000002 HSG80 lun(d100:3) (SP_MONITOR:
MonitorSubsys)
```

This digit can have one of three values:

0—Everything is fine.
1—A LUN state changed from bad to good.
2—A LUN state changed from good to bad.

The details about the failure of the LUN follow in parentheses, in the format:

```
virtual_disk:state
```

where *virtual_disk* is the unit number of the virtual disk and *state* is any of the following:

0—Good.
1—Reduced.
2—Reconstructing.
3—Failed.

In this example, logical unit D100 failed.

In most cases, the RaidManager sends at least two consecutive email messages. The first message is always in the form:

```
---------------
From RaidManager Tue Oct 6 16:09:37 1998
Date: Tue, 6 Oct 1998 16:09:37 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!

Hostname: Suncity

WARNING: - A RAID system change has been detected: Suncity HSG80
OVRL=1 (SP_MONITOR: MonitorSubsys)

End Of Automatic Message.
-------------
```

The text of the second message will be similar to the following (depending on the error):

```
---------
From RaidManager Tue Oct 6 16:09:37 1998
Date: Tue, 6 Oct 1998 16:09:37 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!

Hostname: Suncity

WARNING: - Suncity HSG80 12000000000 HSG80 disks(disk10200:1
disk10300:2) (SP_MONITOR: MonitorSubsys)

End Of Automatic Message.
-------------
```

Note: This example shows that disk10200 went from bad to good, and disk10300 went from good to bad.

Using the Storage Window

5

Why Use the Storage Window?

The Storage window allows you to configure your storage subsystem. Use the Storage window to do the following:

■ Configure the properties of the controller, host ports, and cache

■ Create the following RAID types:

— Striped device group (RAID 0)

— Mirrored device group (RAID 1)

— Striped mirrored device group (RAID 0+1)

— Striped parity device group (RAID 3/5)

— Individual device [JBOD (Just a Bunch of Disks)]

■ View the status of virtual disks, communications LUN, and battery

Storage Window Display

HP recommends that you use a minimum of SVGA (800x600) display resolution. The Storage window requires a minimum amount of screen space to properly display its contents. When you use VGA display resolution, screen space becomes more limited.

If you must use VGA resolution, consider the following suggestions:

■ You may not be able to see the scroll bars on the bottom of the display. You can use the Storage window's menu settings to remove the toolbar from the display to make room for the bottom scroll bars.

■ If you are using the Client with a 24-device, high-availability enclosure, it may be easier to configure the subsystem if you set the system type to Generic for configuration purposes. Return the setting to High-Availability 24-Device Pedestal for monitoring and viewing.

Configuring a Controller

Your controller's operating parameters are stored under six tabs in the Controller Properties window, which you can access by one of two methods:

■ Double-clicking a **controller icon** in the Storage window

■ Right-clicking a **controller icon** in the Storage window and choosing **Properties**.

A change in some controller settings requires that you restart. The program prompts you to confirm the restart.

Modifying the General Properties of the Controller

The properties of the top and bottom controllers, such as type, serial number, SCSI address, firmware revision, hardware revision, and common parameters are stored under the General tab.

To configure the general properties of the controller, click the **General** tab. Refer to step 12 for a description of each general property.

Table 12: General Tab in the Controller Properties Window

What You Can Change	Description
Enable Command Console LUN alias	The Command Console LUN (CCL) appears as a virtual device to your host. If your host allows device aliases, you can assign an alias to the CCL.
	To use this feature, enable your CCL. Click the Enable box and enter a name in the text box. Ensure the format of the name follows the guidelines for your operating system.
Allocation class	Use extreme caution when changing the setting of this field.
	⚠ **Caution:** Changing the setting of the allocation class of your controller may cause data corruption and your host system may require restarting.
Enable autospare	If a replacement policy is in place and autospare is enabled, a failed drive will look for a spare drive. Check your legend for icons that show the status of this process. To determine whether a replacement policy is set, click the Settings tab in the Virtual Disk Properties window.
	Note that this option is not available on devices using RAID 0 or JBOD storage.
Time and date	The controller uses the internal clock to time stamp event logs and status messages.
	Both the time and date fields must have values to change either parameter. You cannot leave the date field blank.
Enable remote copy mode	Enable remote copy mode activates remote copy for a controller pair (subsystem). This feature requires you to first enable remote copy mode for the controller.
	To disable this feature, first remove all remote copy sets and remote copy set connections from the Connections tab of the Controller Properties window.
Remote copy mode	The Remote copy mode field displays the name assigned to the controller pair when remote copy was enabled. To change the value for this field, you must first delete all existing remote copy connections from the Connections tab of the Controller Properties window.

Viewing the Properties of the Host Port

The Host Ports tab displays the following information:

■ Port ID

■ Fibre Channel profile

■ Requested topology

■ Actual topology

■ Remote copy mode name that was assigned when remote copy was enabled

Modifying Properties of the Cache

The Cache tab provides the following information:

■ Write cache size

■ Cache version

■ Cache status

■ Unflushed data in cache

■ Cache flush time (seconds)

■ Cache uninterruptible power supply (UPS) settings

■ Enables mirrored cache

Confirm the following:

■ `Cache flush_time`: (seconds): is 10

■ No UPS is selected

Note: The controller requires that read-ahead cache mode is enabled before you can enable write-back cache mode.

Viewing the Communications LUN

Click the Communications LUN tab to display the properties of the CCL. If the CCL (SWCC virtual LUN) is disabled, the options under this tab are unavailable. For more information about Floating and Fixed options and about the CCL, see Appendix A.

Modifying the Connection Properties

Click the Connections tab to modify the connection properties, shown in Table 13.

Table 13: Connections Tab in the Controller Properties Window

What You Can Change	Description
Connection name	The connection name is a unique string of alphanumeric or punctuation characters that identifies a connection between a host bus adapter and the HSxxx controller. The host performs a Fibre Channel bus scan when it receives notification of a change to the fabric. As part of its device discovery process, the host then identifies the HSxxx as a SCSI device and login to the HSxxx controller. As the host performs the logs into, the HSxxx controller allocates an entry in the host connections table and assigns a connection name to the new connection. Subsequent logins by the host will use this same connection name and entry.
	Controller-produced connection names take the form "!NEWCONN*nn*", where *nn* is a two-character, decimal integer. This string format is not allowed for user-created connections.
Operating system	You can set your controller to operate with a variety of operating systems. Refer to the release notes for operating systems compatibility.
Unit offset	A decimal integer used to determine the LUN address of a virtual disk on a specific connection. Offsets can range from decimal 0-199.
Delete	You can delete a connection by placing a check in the delete box. After placing a check in one or more of the boxes, click the **Delete** button. A confirmation dialog window opens listing the connections to be deleted. Click the **OK** button to delete. A confirmation message is displayed when the deletion is complete.
	Note: Only connections on the current page can be deleted (a maximum of 8).

Viewing Properties of the Battery

The Battery tab provides the following information:

■ The state of the battery

■ The expiration date of the battery

Creating Virtual Disks

You can use the Virtual Disk Wizard to create different types of logical storage units (called virtual disks) on your subsystem.

You can create the following types of virtual disks:

■ Single-device virtual disks (JBODs)

■ Striped virtual disks (RAID 0)

■ Mirrored virtual disks (RAID 1)

■ Striped mirrored virtual disks (RAID 0+1)

■ Striped parity virtual disks with parity across all drives (RAID 3/5)

Note that the capacity of the smallest member, not the largest, determines the maximum capacity of RAID-based virtual disks.

■ The maximum capacity of RAID 0 virtual disks is equal to the number of members times the capacity of the *smallest* member.

■ The maximum capacity of RAID 1 virtual disks is equal to the capacity of the *smallest* member.

■ The maximum capacity of RAID 0+1 virtual disks is equal to the number of members in one stripe times the capacity of the *smallest* mirrorset member.

■ The maximum capacity of RAID 3/5 virtual disks is equal to the number of members minus one times the capacity of the *smallest* member.

Before you can create virtual disks from a physical device, your controller must know of the device. You can add devices online without restarting the controller.

This procedure describes how to add a physical device before you create a virtual disk.

To add a physical device and then create a virtual disk, follow these steps:

1. From the Navigation window, open a Storage window within a desired subsystem.

2. Click **Storage > Device > Add** in the Navigation window.

3. If there is no user input in the Storage window within an hour, you are prompted to enter a password. Type the SWCC password in the Security Check window and click **OK.**

   The SWCC password was created when you installed the Agent. To change the password, open the Agent Configuration utility on the agent system (host).

4. Select the type of virtual disk that you want to create, and click **Next** in the **Add Virtual Disk Wizard – Step 1 of 5** window.

5. Select the physical devices to include in the virtual disk by clicking them in the **Available Storage** field in **Add Virtual Disk Wizard – Step 2 of 5** window.

   As you click a physical device, it is added to the **Selected Devices** field. If you selected JBOD in the previous step, you can select only one device.

6. Click **Next.**

   You see the **Add Virtual Disk Wizard – Step 3 of 5** window.

7. Type the capacity of the virtual disk in the **Capacity for Virtual Disk** field, and click **Next** in the **Add Virtual Disk Wizard – Step 3 of 5** window. This window provides you with the maximum and minimum megabytes that you can choose for a capacity.

8. Type the unit number, operating parameters, and options for the virtual disk, and then click **Next**. To save the controller configuration, choose the **Save controller configuration to virtual disk setting** in the **Add Virtual Disk Wizard – Step 4 of 5** window.

Note: Saving the configuration to disk in a redundant controller configuration is not supported and can cause unexpected controller behavior.

Virtual disks based on partitions on any container are all closely related because they all share the same target and operating parameters of the container. If you change any of this information for one partition on the container, all the partitions on that container are changed.

---

9. The **Add Virtual Disk Wizard – Step 5 of 5** window – displays the selections that you made in steps 1-4.

10. If you are satisfied with your choices, click **Finish** to create the virtual disk.

> **Note:** The time required to initialize a virtual disk depends on the number of members and its size. During initialization, the virtual disk is unavailable for I/O. You should not use the virtual disks until initialization is complete.

After creating a virtual disk, you must perform additional steps to properly configure your operating system. See "Configuring the Operating System to Recognize Virtual Disk Changes", page 77, for more information.

Deleting Virtual Disks

The virtual disks in your subsystem are logical units that contain your user data. Although virtual disks do not exist in a physical sense, their logical structure ties together the physical pieces of your data spread across the members. When deleting a virtual disk, use extreme caution in order to prevent deleting valuable user data.

To delete a virtual disk:

1. Do one of the following:

   — From Windows NT 4.0, use Disk Administrator to delete the partition.

   — From Windows 2000 and Windows Server 2003, use Disk Management to delete the partition.

   — From UNIX or OpenVMS, ensure that any file systems that were mounted on the device are unmounted and removed. If the drive was part of a logical volume, remove the device from the logical volume system.

2. Click the icon of the virtual disk that you want to delete.

3. Choose **Storage > Virtual Disk > Delete** in the Storage window.

4. If the Client prompts you for your password, enter it.

5. When the Client prompts to confirm the change, click **Yes** to continue. The Client deletes your virtual disk from your configuration and refreshes the Storage window.

After deleting a virtual disk, you must perform additional steps to properly configure your operating system. See "Configuring the Operating System to Recognize Virtual Disk Changes", page 77, for more information.

Modifying Virtual Disks

You can modify the characteristics of your virtual disks in two ways:

■ Change their operating characteristics

■ Remove their members

> **Caution:** Use extreme caution when modifying the characteristics of a virtual disk. You may be putting valuable user data at risk.

You can change the characteristics of a virtual disk by accessing its property sheets.

To access the property sheets of a virtual disk, refer to and do one of the following:

— Double-click the virtual disk icon .

— Right-click a virtual disk icon and choose **Properties**.

Table 14: Virtual Disk Properties Window

Tab	Information
General	Lists the characteristics of the virtual disk.
Settings	You can change chunk size, reconstruction rate, replacement policy, and maximum cached transfer blocks. You can also enable or disable write-back cache by clicking the checkbox. Click **OK** to save the changes and to exit. **Note:** The controller requires that read-ahead cache mode is enabled before you can enable write-back cache mode.
Membership	Displays the member devices. Can view a device by name and its current state, channel, target, and capacity.

Configuring the Operating System to Recognize Virtual Disk Changes

The Client does not perform all of the system configuration necessary to make your subsystem's virtual disks visible to the user in the operating system.

When you create or delete virtual disks using either the Command Line Interface (CLI) or Client, you are adding or removing "disks" in the subsystem in a manner similar to plugging or unplugging physical disk drives on the host bus. In either case, there are certain operating system configuration actions you must perform to make these "disks" visible or invisible to the operating system's file system.

Windows NT/Windows 2000/Windows Server 2003 Configuration

On a Windows NT, Windows 2000, or Windows Server 2003 host, after you create or delete a virtual disk, you must perform the following steps to properly configure the file system to recognize your changes:

1. Start the host system. This action has the effect of forcing the Disk Administrator or Disk Management to recognize added virtual disks as raw disks, available for use. Deleted virtual disks are no longer present.

2. Create file system partitions on your disks. When you create a virtual disk in the controller, you can partition it at the controller level in any way you wish as long as you create at least one partition per disk. Each of the controller-level partitions you create becomes a virtual disk, visible to the host. In Disk Administrator, you must create partitions on these newly added virtual disks at the Windows NT file system (NTFS) level.

3. After you create partitions on your drives in Windows NT, Windows 2000, or Windows Server 2003, the file system assigns each drive a unique drive letter. Make a note of the drive letters assigned.

4. Format your disks. You must format each newly added disk.

5. Start the Agent Configurator by double-clicking its icon in the Command Console Start Menu group.

6. Navigate through the menus until a popup appears, prompting you to scan your subsystems. Click **Yes** to perform the scan and display a list of subsystems.

7. Make sure that the access device you have been using for your subsystem still exists. If you inadvertently deleted it, you must assign another device in its place. If no access device exists, the Client cannot communicate with your subsystem unless the CCL is used.

8. Click **Next** until you can exit the configurator.

9. Choose the **Services** option in the **Windows Control Panel** for Windows NT, or Computer Management in Administrative Tools for Windows 2000 and Windows Server 2003.

10. Scroll down to highlight the **Steam** entry.

11. Click **Stop** and wait for a prompt indicating that the service is halted.

12. Click **Start** and wait for a prompt indicating that the service is started.

13. Exit Control Panel.

    Windows NT, Windows 2000, and Windows Server 2003 now recognizes any changes you made in your virtual disk configuration.

UNIX-Based Configuration

On a UNIX-based host, after you create or delete a virtual disk using the Client or CLI, you must perform the following steps to properly configure the UNIX file system to recognize your changes:

1. Restart the host system. This action has the effect of forcing the file system to recognize added virtual disks as raw disks available for use. Deleted virtual disks are no longer present.

2. (Optional) Create file system partitions on your disks. When you create a virtual disk in the controller, you have the option to partition it at the controller level in any way you wish. Each of the controller-level partitions you create becomes a virtual disk, visible to the host.

3. Afterward, if you desire, you can partition these newly added virtual disks at UNIX's file system level. Use the appropriate commands for your operating system version to perform this task. Once you have partitioned your drives in UNIX, the file system assigns each drive a unique drive identifier.

4. Stop and Restart the Agent. Using the Agent configuration script, you must stop and restart the Agent running on your UNIX host, using the configuration program. In the program, you must choose the option to create a new storage.ini file. This action updates the Agent to recognize any virtual disk changes you have made.

Setting Passwords and Security Options (Network Only)

Password security prevents unauthorized users from changing or removing storage configurations. In SWCC, the following operations require a password:

■ Changing controller configuration

■ Changing virtual disk configuration

■ Changing device settings

Security Options

The two security options, View Only and Make Changes, are available from the Storage Window Options menu.

Password Security

You create a password when you install the HS-Series Agent on a system. The password is encrypted and stored in the file where the Command Console Agent resides. To set or change a password, use the Agent Configuration menu.

Command Console allows a user with a valid password to make configuration changes for one hour. If an hour elapses without user input, the Command Console resets itself to View only. Any configuration change resets the timer and keeps the current password active for one hour.

Managing and Creating Spare Devices

Making a spare device part of a virtual disk lets you protect the integrity of the RAID setup. A spare is especially important for virtual disks that have RAID requirements of two or more devices. If one device fails, the virtual disk instantly and automatically activates the spare device as a replacement.

A spare works as follows: if a device fails in a RAID 1, RAID 0+1, or RAID 3/5 virtual disk, the spare automatically replaces the failed device and the controller reconstructs all virtual disks of which the failed device was a member.

After the controller writes data to a spare, the spare becomes part of the same device group in which a device failed.

Creating a Spare Device

To create a spare device:

1. In the Storage window, click the device that you want to use as a spare. For an automatic failed drive replacement, the device must be available and have a capacity equal to or greater than the lowest capacity drive in the group.

2. From the Storage menu, choose **Device**, and then choose **Make Spar*e***.

Clearing Failed Devices

In the Storage window, the icon of a failed device is displayed with an X covering it.

To clear the failed device:

1. From the Storage menu, choose **Device**.

2. Then choose **Delete**.

Using Configuration Files

You can use a configuration file to save a subsystem configuration and view or reconstruct it at another time. You can revert to a saved configuration at any time. The Client reads the configuration file that you choose and sets up your subsystem accordingly.

Saving Configuration Settings to a File

To save the configuration settings for a subsystem:

1. Click **Storage > Controller Configuration > Save**.

2. Follow the instructions on the screen.

The current configuration settings, including caches, LUNs, host port, and stripe size, are saved to a file at the location that you specify.

Restoring Configuration Settings from a File

You can restore your entire subsystem from a saved configuration file. The Client can restore your subsystem only if the configuration file corresponds to your subsystem's hardware configuration and if all of the controllers are attached to a serial connection.

> △ **Caution:** Be aware of the configuration information in the configuration file that you choose. If you choose a file that is incompatible with the current configuration of data on your devices, you put your data at risk.

To restore your subsystem from a saved configuration file:

1. Choose one of the displayed options:
   — If you need to reconfigure a failed controller that has existing virtual disks, choose **Load configuration only**. The Client recreates your virtual disks, but it does not initialize them. Your data is not overwritten.
   — If you are configuring a new system, choose **Load configuration and initialize virtual disks.**

2. Click **OK**.

3. When the Open dialog box displays, specify the location (path) and file name in the text box, and then click **Open**.

The configuration settings, such as caches, LUNs, host port, and stripe size, are restored.

> ⚠️ **Caution:** If the original hardware and connections are replaced or are not saved before making new changes, you cannot restore the original configuration settings.

Understanding the Icons

You can obtain a definition of the icons by clicking **View > Legend** in the Storage window.

The Storage window provides detailed information in both physical and logical views of a subsystem in the Storage window. In each view, icons represent device and virtual disk states. These icons change to indicate status. An X through a device indicates device failure. The Storage window status bar indicates power, fan, temperature, and battery states.

Table 15: Description of Icons in the Storage Window Status Bar

Icon	Description
	Indicates that the cabinet fans are all operating normally
	Indicates that there is a problem with the cabinet fans
	Indicates that the cabinet temperature is within its acceptable range
	Indicates that the cabinet temperature is out of its acceptable range
	Indicates that all power supplies are operating normally
	Indicates that the cache backup batteries are fully charged and operating normally
	Indicates that there is a low charge condition on the cache backup batteries
	Indicates that the cache backup batteries have failed or are discharged

CLI Window

The CLI is a text-based interface utility for monitoring and configuring your storage subsystem. Because the configuration of the storage subsystem can be changed using CLI commands, HP recommends that you allow CLI access only to users who are familiar with CLI operation.

The CLI window, as shown in Figure 11 has a command-entry area and a command-response area below it. You can enter commands in the command-entry area, and the controller responds with the results of the entry in the response area.
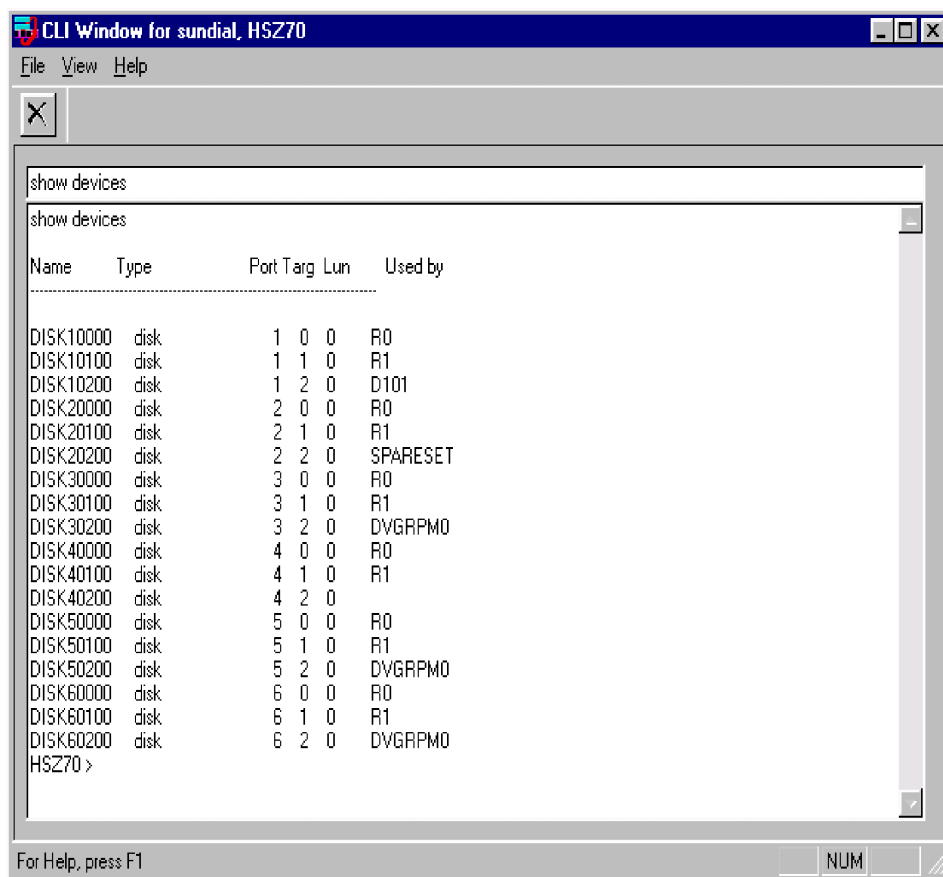
Figure 11: CLI Window

CLI Functions

There are some functions available in the CLI that are not available in SWCC.

■   If you wish to use your controller's multiple-bus failover mode, you must enable and control that function with the CLI.

■   If you wish to use virtual disk preferences in multiple-bus failover mode, you must set your virtual disk preferences with the CLI when you set the failover mode.

Integrating SWCC with Insight Manager

6

You can use the HSGxx Storage windows within Insight Manager V4.23 or later to monitor and manage the controllers. If your HSGxx controller uses Array Controller Software (ACS) V8.5 or later, you need to install the integration patch (HSG80 Shim). HSG80 Storage Window V2.4 is required to run the integration patch.

Installing the Integration Patch

To install the integration patch:

1. Verify that the HSGxx Storage Window for ACS V8.5 or later is installed by looking in Add/Remove Programs. Click **Start > Settings > Control Panel > Add/Remove Programs**.

2. Verify that the HSG80 Storage Window V2.4 is installed by looking in **Add/Remove Programs** *(HP StorageWorks HSG80 V2.4).*

3.   Verify that Insight Manager V4.23 or later is installed.

4. Install the integration patch from the Solution Software CD-ROM by double-clicking **setup.exe** in the top-level directory. The SWCC Setup window opens.

5. Choose HSG80 Controller Shim. If you do not have the HSG80 Storage Window V2.4, also choose HSG80 Controller.

6. Click **Next.**

The patch is installed in the same location as the original SWCC installation.

Integrating the HSGxx Storage Window with Insight Manager

To open an HSGxx Storage window:

1. Look in **Add/Remove Programs** in the Control Panel to verify that the following are installed:

   — The HSGxx Storage Window for ACS 8.5 or later (required to open the correct Storage Window for your firmware).

   — The HSG80 Storage Window 2.4 *(HP StorageWorks HSG80 V2.4)*. The integration patch uses files in this program.

   — Insight Manager 4.23 or later.

   — Insight Manager integration patch *(HSG80 Insight Manager Shim)*.

2. Verify that you have installed the Insight Manager Agent and the StorageWorks Command Console HS-Series Agent on the same computer.

3. Add the name of the client system running Insight Manager to the Agent's list of client system entries and choose SNMP as a notification scheme.

4. Open Insight Manager.

5. To open the Server window, click the device that you want to observe in the Insight Manager Navigation window.

6. Click **Mass Storage** in the Server window. The Insight Manager Navigation tree is displayed.

7. Expand the Navigation tree to display **Storage System Information**.

8. Double-click **Storage System Information**. You are given the status of the system.

9. Click **Launch.** The Storage window opens.

Insight Manager Unable to Find the HSGxx Storage Window

If you install Insight Manager before you install SWCC, Insight Manager will not be able to find the HSGxx Storage Window.

You can correct the problem by following these steps:

1. Click **Start > Settings > Control Panel** and then double-click the **Insight Agents** icon.

   A window opens showing you the active and inactive Agents under the Services tab.

2. Highlight the entry for **Fibre Array Information** and click **Add**.

   The Fibre Array Information entry is moved from Inactive Agents to Active Agents.

Removing the Integration Patch Disables Storage Window

If you remove the integration patch, HSG80 Storage Window V2.4 will not work. You will have to reinstall HSG80 Storage Window V2.4. The integration patch uses some of the same files as the HSG80 Storage Window V2.4.

Troubleshooting

7

Troubleshooting Connection Problems

SWCC is a TCP/IP socket-based application. As a result, SWCC requires that each node running a SWCC Client or Agent has access to a valid hosts file or Domain Name Service (DNS) server. Minimally, the valid hosts file must include the system itself and all systems running the SWCC Client and Agent.

Invalid Network Port Numbers During Installation

During the Client or Agent installation, you may experience an error if the installation program cannot find an acceptable pair of network port numbers.

Your Client uses Windows sockets (sometimes called "network ports") to communicate with its Agents. The socket numbers at the Client and Agent ends must match for network communication to occur.

In Windows NT, Windows 2000, and Windows Server 2003, the socket numbers are assigned in the services file in the `\winnt\system32\drivers\etc` subdirectory. In UNIX-based systems, the socket numbers are assigned in the services file in the `/etc` subdirectory. In the unlikely event that you experience a conflict with the socket numbers, you may edit the file manually.

There are two default socket numbers, one for Command Console (4998) and the other for the HS series Client and Agent (4999). If you are installing the Client or Agent and these numbers are already taken by another application, the installation program prompts to warn you that you must choose another pair.

To choose another pair for the Client, open the file containing the sockets in an ASCII editor. Choose two numbers above 1023 that are not already used in the file, and add the following two lines:

```
spgui number1/tcp # StorageWorks® Command Console

spagent  number2/tcp # StorageWorks® Command Console
```

Note that the port numbers that you choose must match the port numbers used by all of the Clients that connect to your Agent.

Network Port Assignments for UNIX-Client/Server Systems

A UNIX host may use Network Information Services (NIS) to serve the services file containing its network port assignments.

The Agent must use the services file to determine which network ports to use. Because of this requirement, you may need to configure your system so that the Agent can access the proper services file.

You have two options to prevent a conflict between the two possible locations of the services file. See your particular Agent guide for more information.

DHCP and WINS

SWCC does not support the DHCP or the WINS; however, you can still use these protocols on systems that do not run the Command Console.

First, verify that your network is running:

■ For Windows NT, Windows 2000, or Windows Server 2003, run `netstat` at the command prompt on the Agent and check the active TCP/IP connections.

■ For UNIX, run `netstat` with the correct options. Reference `netstat` man pages in UNIX help information.

■ For other operating systems, refer to the operating system documentation.

To determine whether your system is using DHCP or WINS on Windows NT 4.0:

1. Right-click **Network Neighborhood** on the desktop.
2. Select **Properties**.
3. Click the **Protocols** tab.
4. Select **TCP/IP**, and then click **Properties**. The Microsoft TCP/IP Properties window opens.

To determine whether your system is using DHCP or WINS on Windows 2000 or Windows 2003:

1. Right-click **My Network Places** on your desktop.
2. Select **Properties**.
3. In the **Network and Dial-up Connections** window which opens, right-click the connection to be used by SWCC.
4. Select **Properties**.
5. Select **Internet Protocol (TCP/IP)**, then click **Properties**.

The Microsoft TCP/IP Properties window opens.

Connecting Via the Host SCSI Port

The Client may indicate that it cannot find your subsystem if you attempt to connect with the host SCSI port by using Windows NT, Windows 2000, or Windows Server 2003 in either of the following situations:

■ An HP StorageWorks controller subsystem is not connected to the host.

■ An HP StorageWorks controller subsystem is connected to the host, but the subsystem uses SCSI-2 mode and has no virtual disks configured on it with CCL disabled.

If you are using SCSI-2 mode and Windows NT, Windows 2000, or Windows Server 2003, you must disable the Command Console LUN and create a virtual disk by using a serial connection. See "Enabling and Disabling the CCL", page 107, for more information.

Because the Agent uses a SCSI host bus connection to its subsystems, the same rules mentioned above also apply.

"Access Denied" Message

This section describes some common reasons for a Client to receive an "Access Denied" message when you add an agent system to the Navigation tree.

Aliases Not Checked

Ensure that the Agent's host system is configured to recognize the Client by its assigned name rather than by an alias. If the host system has been configured to recognize the Client by an alias, remove the alias from the system's hosts file.

When SWCC Agents scan the Client authorization list, they do not check aliases. SWCC will not scan the hosts alias list to verify if an alias matches the Client authorization list.

Entry in the Client Authorization List Does Not Match

You may see an "Access Denied" message if the name of the client system that you entered in the Agent configuration utility does not match the one for DNS or the one in the agent system's hosts file. The hosts file on Windows NT 4.0, Windows 2000, and Windows Server 2003 is at `\winnt\system32\drivers\etc`.

Your system may be configured to do one the following:

■   Check local hosts file first, and then go to DNS (most common setup for Windows NT, Windows 2000, and Windows Server 2003).

■   Go to DNS first, and then check local hosts file.

■   Ignore DNS even if configured.

■   Ignore the local hosts file.

To determine your system configuration for Windows NT:

1. Right click **Network Neighborhood** (on the desktop).

2. Choose **Properties**.

3. Click the **Protocols** tab.

4. Choose **TCP/IP**, and then click **Properties**.

    The Microsoft TCP/IP Properties window opens.

5. Click the **WINS Address** tab. If your computer uses DNS, the Enable DNS for Windows resolution option is selected; you do not need to have Enable LMHOSTS Lookup selected.

    If WINS servers are available on the network, the LMHOST file can be used. SWCC does not support WINS.

6. To determine the IP address for the system, click the **IP Address** tab in the Microsoft TCP/IP Properties window.

7. To determine the full name of the system, click the **DNS** tab.

To determine your system configuration for Windows 2000, and Windows Server 2003:

1. Right-click **My Network Places** on your desktop.

2. Select **Properties**.

3. In the **Network and Dial-up Connections** window which opens, right-click the connection to be used by SWCC.

4. Select **Properties**.

5. Select **Internet Protocol (TCP/IP),** then click **Properties**.

The **Internet Protocol (TCP/IP) Properties** window opens.

6. Click **Advanced**.

The **Advanced TCP/IP Settings** window opens.

7. Click the **WINS** tab.

8. Click the **WINS Address** tab. If your computer uses DNS, you do not need to have **Enable LMHOSTS Lookup** selected.

Note: If WINS servers are available on the network, the LMHOST file can be used. SWCC does not support WINS.

---

9. Check the **General** tab in the **Internet Protocol (TCP/IP) Properties** window to determine the IP address for the system,.
10. Click the **DNS** tab in the **Advanced TCP/IP Settings** window to determine the full name of the system.

For other operating systems

Generally, the entry for an Agent in the Client authorization list must match what gethostbyaddr(<client IP address>) returns in the hosts agent h_name field if gethostbyaddr(<client IP address>) is executed on the Agent system. If the hosts files names on all systems are not identical, the h_name returned may vary on different Agent systems. For example,

    xxx.xxx.xxx.xxx   client.*somewhere*.com   client

returns client.*somewhere*.com in the h_name field, but

    xxx.xxx.xxx.xxx   client   client.*somewhere*.com

returns client in the h_name field.

The best way to determine what to use for a Client name in the Client authorization list is to write a program that runs on the Agent system and prints the h_name field returned by gethostbyaddr(<client IP address>).

Multiple Agents

If the Agent system is running multiple SWCC Agents (for example, to support different controller types), the client system must be authorized for all Agents. If the client system is missing from any authorized Client list of an Agent, that Agent cannot be added to the Navigation tree.

Adding New System by Using Internet Protocol Address May Cause Client to Stop Responding

The SWCC Client may stop responding if you attempt to add a system by using the agent system's IP address rather than its node name. This occurs when the client system does not have a DNS server configured that knows the agent system, and the agent system is not included in the client system's hosts file. To correct this situation, add the agent system to the hosts file on the client system.

If you receive an "Invalid host" or "Host not known" message when you attempt to connect to an agent system, do not enter the IP address. Correct your DNS server configuration. If it is correct, confirm that the DNS server knows the agent system. If you are not using DNS, verify the agent system is in the client system's hosts file.

"No Agent Running" Message When Adding System to the Navigation Tree

While attempting to add a new system to the Navigation tree, you may see the message "No Agent running on specified system." This message may appear for several reasons. The following are the most likely:

■   The wrong system name was entered.

■   The Agent was not installed on the entered system.

■   The Agent was installed on a system that stopped functioning.

■   Client and Agent port names and numbers in the services file may not match. This may occur if the default value for an SWCC port was already in use. See for more information.

■   The specific Client required to support an Agent is not installed. For example, if the Agent system has only a KZPCC Agent and the client system has only an HSZ22 Client, the "No Agent Running" message is displayed.

    To verify that there is Client support for an Agent, look at the following registry key:

    ```
    HKEY_LOCAL_MACHINE\Software\DigitalEquipmentCorporation\Command
    Console\AppletManager
    ```

    You should see a series of keys for supported products.

■   Make sure the system names used for the Client and the Agent match exactly. As a general rule, use lowercase letters when entering names.

■ You entered the host name in the `\winnt\system32\drivers\etc\hosts` file. The host name is not required here, but TCP/IP looks at this file first to resolve a host name.

Troubleshooting the Client

Authorization Error When Adding an Agent System

If you receive an authorization error when you add an agent system to the Navigation tree, your client system may be missing from the Agent's list of client system entries. If you have more than one type of Agent installed on that agent system, the name of your client system is displayed on each Agent's list of client system entries.

Cannot Open Storage Window

If you cannot open a Storage window from the Navigation tree or in standalone mode, the client system access option for the subsystem to which you want to connect is probably set to Overall Status (0), disabling access to the Storage window.

Client Hangs When LUN Is Deleted

If you delete the LUN that is used by the communication drive, you cannot communicate with the controller. You must assign another LUN to the monitored subsystem before deleting the original LUN.

If you disable the Command Console LUN, the Client may lose its connection with the subsystem. If you need to disable the communications LUN, first assign another LUN as the communications LUN.

CLI RUN Commands

Do not issue RUN commands in the CLI window. Instead, issue RUN commands from a maintenance terminal connection.

Event Notification for Subsystems Connected to a Client System

To use the event notification features, an Agent must be installed and running. Create a local network connection by running the Client and Agent on the same Windows NT/2000/Windows Server 2003 host computer. Install each component as if the Client were running on a remote system.

Invalid or Missing Fault Displays and Event Logs

Invalid or lost notifications may occur when the client system loses connection with a subsystem. The client system receives notification about most of the changing subsystem faults at monitored intervals. If the client system no longer receives notification about subsystem faults, then changes to that subsystem will not appear in the client system's Navigation tree, Storage window (if applicable), Fabric window (if applicable), and Event Viewer.

For example, while client system's connection with a subsystem is broken, you will not receive event logs about that subsystem, except the lost connection notification.

The following list describes common causes for lost connections. After you fix the physical and/or software problem that is listed below, you need to close and reopen the Storage window for that subsystem to get its latest status.

- RAS connections—Remote Access Service (RAS) connections are not full-time. If no RAS connection exists, events are not logged to the Event Viewer Application Log.

- Serial controller connections—There may be a bad or missing serial cable. To correct this situation, replace or plug in the cable.

- Network connections—Agent may be missing or not running.

- Network connections—There may be network discontinuity.

- The Agent may not be properly configured for a client system.

- If your setup includes a controller, the controller may have halted, reset, or hung. To repair the situation, restart or replace the controller.

- If your setup includes virtual disks, the virtual disk used for communicating with the subsystem is no longer available.

Pager Notification Continues After Exiting the Command Console Client

You may have noticed continuous pager notification in response to subsystem faults, even though you have exited the Command Console Client. This behavior is normal.

AES runs as a service under Windows NT, Windows 2000, and Windows Server 2003. It continues to run after you exit the Command Console Client. AES communicates with Agents and activates paging when a subsystem event occurs.

To stop pager notification, stop AES. For information about stopping AES, see Chapter 2.

Reconfiguration After Controller Replacement

If you replace a controller in your subsystem, you must reconfigure your Agent's storage list to match the new hardware.

Some Graphics Do Not Scale Well with Large Fonts

Display small fonts when using the Client. Some graphics do not scale as well if large fonts are used.

Starting Client from the Command Prompt

To start the Client with network connections from the command prompt, enter the following at the command prompt on the Client system:

```
\path_to_client_directory\swcc.exe -d your_host_system
your_host_subsystem
```

where -d your_host_system your_host_subsystem is an optional set of parameters that enables you to specify a system and a subsystem to start the Client.

For example:

```
C:\>\Program Files\Compaq\SWCC\swcc.exe -d hostsystem subsystem
```

If you specify these parameters when the Client opens, the system is selected and the subsystem is displayed in the Storage window. If the Client is not already aware of the system and the subsystem, it adds them to the Navigation tree.

Warning Message Windows

You may see warning messages, such as "Command Execution Error" along with detailed information. These messages indicate problems with the controller, rather than with the software. The controller is responding to problems in parsing and executing commands from the Client and Agent.

Virtual Disk Recovery from a Configuration File

If you delete a virtual disk, all the member drives are re-initialized and data is lost. You cannot restore a virtual disk's data by changing the configuration. A configuration file contains information about only the structure of a virtual disk - it does not store data.

Troubleshooting the HS-Series Agents

This section describes how to troubleshoot the HS-Series Agents.

Agent Sensitive to Alphanumeric Names

The Agent may not accept some alphanumeric name forms, particularly those with embedded underscores. If you experience difficulties with a node name, change the node name to one that the Agent accepts.

Invalid Cache Errors

Your controller module, cache module, and subsystem contain the configuration information that is used for synchronization. This configuration information is called metadata. The firmware reports an invalid cache error on an affected controller if there is a mismatch between the metadata in the controller module and a cache module containing unwritten data. This mismatch may result in the loss of the unwritten cache data if the error is not cleared properly.

You may lose valid data if you clear unwritten cache data. The Client displays a message and prompt box when an invalid cache error occurs. Use the CLI window to clear unwritten cache data as the error is cleared. For information about how to clear unwritten cache data, see the "Invalid Cache Errors" topic in online Help.

Cluster Integration for the HS-Series Agents

This section describes how to integrate a Windows NT cluster with SWCC.

How to Integrate SWCC with Windows NT

When you integrate a Windows NT cluster with SWCC, you can configure and monitor a subsystem within the cluster environment. You need the following to perform cluster integration:

■   A valid, working stable cluster

■   An Agent installed on a disk that is on a non-shared SCSI bus

■   An Agent on each cluster node of the cluster

To integrate a Windows NT cluster with SWCC:

1. Click **Settings** under the **Start** menu, and then click **Control Panel**. Double-click **Services**.

    The Services window opens.

2. Choose **Steam** from the drop-down list for the Service field, and then click the **Stop** button. Steam, which stands for StorageWorks Enterprise Array Manager, is the name for the HS-Series Agent service. This action stops Steam, and its status no longer displays as Started in the Services window.

3. Click **Startup**. A smaller **Services** window opens.

4. Choose **Manual**, and then click **OK** to disable the automatic start of the service.

    You are returned to the main **Services** window.

5. Click **Close** to exit the Services window.

6. Repeat steps 1-5 for each cluster node.

7. Click the **Cluster Administrator Utility** entry under the **Administrative Tools** group.

    The program's main screen opens.

Note: Microsoft develops Cluster Administrator Utility. For further information about the software, see the appropriate documentation.

To complete the Cluster Administrator Utility information:

1. Click your cluster group.

   The resources in your cluster group appear.

2. Verify that your cluster group includes the quorum disk.

3. Right click the cluster group.

   A drop-down menu appears.

4. Choose **New**, and then **Resource**.

   The **New Resource** window opens.

5. Type the SWCC Agent's name and description. Under **Resource Typ**e, choose **Generic Service** from the drop-down menu. Under **Group**, choose **Cluster Group**.

6. Click **Next**.

   The **Possible Owners** window opens.

7. In the **Possible Owners** field, select the nodes in your cluster where you want the SWCC Agent to run.

8. Click **Next**.

   The **Dependencies** window opens.

9. Choose the following resources: **Cluster IP Address, Cluster Name, and Quorum Disk**.

10. Click **Add** to bring these resources online before starting the SWCC Agent.

11. Click **Next**.

    The **Generic Service Parameters** window opens.

12. Type **Steam** in the **Service Name** field. Leave the **Start-up Parameters** field empty.

13. Choose **Use Network Name** for computer name.

14. Click **Next**.

    The **Registry Replication** window opens.

15. Click **Finish**.

    A message stating that you have successfully created a generic service resource is displayed.

Multiple Communication Lost Messages

On a Client system, AES monitors every agent system that is included in the Client's Navigation tree. If an Agent fails on a system that AES is monitoring, AES generates a page and an event log entry for the Agent at every polling interval indicating that communication has been lost. To stop the page and event log entries, remove the system entry in the Command Console's Navigation tree.

Event Updates

You must manually update any node added to the Navigation tree by using cluster alias and any Storage window that opens from that cluster alias. If you have a pager configured for automatic updating, you must add the individual nodes of the cluster to the Navigation tree.

Multiple Pages

AES may send multiple pages if an Agent moves from a failing node to a working node. When the Agent fails over, a TCP/IP peer reset error may appear in the active Storage window that had been connected to that Agent.

Using the Command Console LUN

<div style="text-align: right;">**A**</div>

This appendix explains how to avoid errors when configuring the Command Console LUN (CCL). Note that Windows NT, Windows 2000, and Windows Server 2003 with SCSI-2 do not support the CCL.

About the Command Console LUN (CCL)

The CCL is a preconfigured virtual LUN, located on controller A, LUN 0. Logical unit numbers (LUNs) are unique identifiers used on a SCSI bus to distinguish between devices that share the same bus. The host uses LUNs to access the storageset.

SWCC sees the CCL as a virtual disk; however, the CCL cannot store information. The CCL is used only as a communication path between the controller and SWCC.

If you enable the CCL, the controller reserves one LUN address for Client or Agent use. The reserved LUN address is stored under the Communications LUN tab. The CCL does the following:

■ Allows the host to recognize the RAID Array as soon as it is attached to the SCSI bus and configured on the operating system.

■ Serves as a communications device for the HS-Series Agent. The CCL identifies itself to the host by a unique identification string. This string, HSG60CCL or HSG80CCL, is returned in response to the inquiry command.

The default state for the CCL is enabled. To determine the address of the CCL, enter the following CLI command:

```
HSG60 > SHOW THIS_CONTROLLER
```

OR

```
HSG80 > SHOW THIS_CONTROLLER
```

Enabling and Disabling the CCL

Do not use the CLI to disable the CCL while SWCC is running. You may lose data and communication between the Client and the Agent. Typically, the CCL remains enabled when you use SWCC. If the Agent system is running Windows NT, Windows 2000, or Windows Server 2003 with SCSI-2, disable the CCL.

To disable the CCL, enter the following CLI command:

```
HSG60 > SET THIS_CONTROLLER NOCOMMAND_CONSOLE_LUN
```

OR

```
HSG80 > SET THIS_CONTROLLER NOCOMMAND_CONSOLE_LUN
```

To enable the CCL, enter the following CLI command:

```
HSG60 > SET THIS_CONTROLLER COMMAND_CONSOLE_LUN
```

OR

```
HSG80 > SET THIS_CONTROLLER COMMAND_CONSOLE_LUN
```

In dual-redundant controller configurations, these commands change the CCL setting on either type of controller. The CCL is enabled only on host port 1. At least one storage device of any type must be configured on host port 2 before you install the Agent on a host connected to host port 2.

Select a storageset that is not likely to change and configure it. The Agent can use this storageset to communicate with the RAID Array. If you later delete this storageset (LUN), the connection between the Agent and the RAID Array is lost.

Using an Initial Configuration

Your storage subsystem may not be configured when you first install it so there may be no virtual disks for Command Console to use. You cannot configure virtual disks because you cannot establish a connection. The CCL allows you to establish the first connection.

Before you run SWCC, enable the CCL.

Note: If you are using SWCC with a SCSI-2 connection with an Agent running on Windows NT, Windows 2000, or Windows Server 2003, you must disable the CCL and create a virtual disk.

Preserving Virtual Disk IDs

In some operating systems, you may disable the CCL to preserve virtual disk IDs. On Windows NT, Windows 2000, and Windows Server 2003 systems with SCSI-2, the LUN appears as a drive letter that you can use only for this purpose. In this case, you must use the controller's CLI window to configure at least one virtual disk for communication before you run Command Console.

Safely Disabling the CCL

To disable the CCL while the Command Console is connected, you need to have at least one virtual disk remaining on your subsystem. Then, exit the Client and stop running the Agent. Disable the CCL from the CLI window. Reconfigure the Agent and the Client to use the remaining virtual disk for communications.

Setting the Fixed/Floating Option

In SWCC, if you select the Fixed option from the Add Virtual Disk wizard, the CCL remains assigned to that location. The Client reserves the address of the LUN, and you cannot use the Add Virtual Disk wizard to create virtual disks.

> **Caution:** The Fixed option works only with the Add Virtual Disk wizard. With CLI you can still overwrite a LUN address assigned to the communications LUN, even if the Fixed option is selected.

If you select the Floating option, you can use the LUN address currently assigned to the communications LUN to create a virtual disk. If you use this address, your controller automatically "floats" the CCL to another address and you lose communication with your subsystem.

To select the fixed/floating option:

1. In the **Device** window, double-click the icon for your controller to display its property sheets. If you have a dual-redundant controller configuration, you can use the property sheets of either controller.

2. Click the **Communications LUN** tab.

   The operating parameters for the communications LUN are displayed.

3. Click either **Floating** or **Fixed** to select it.

> **Note:** Changes to your controller configuration require password access. The program prompts you for the appropriate password on your first attempt to modify the controller.

Cautions When Using the CCL

Be aware of the following cautions when using the CCL:

■   If you select the Client's Floating option and use the CCL address to create a virtual disk, you lose communication between the Client and your Agent. You must reconfigure and restart your Agent to have it recognize either the new CCL address or an existing virtual disk that is used for communication.

■   Within your controller, the CCL always floats to another LUN address if you attempt to use its address to create a virtual disk. The Client's Floating/Fixed option affects only the way the Client presents available LUNs to the Add Virtual Disk Wizard.

■   If you restart your controller, its CCL becomes the lowest available LUN combination that is not already assigned to a virtual disk.

■   If you delete a virtual disk with a LUN address lower than that of the CCL and then restart the controller, the CCL automatically moves to the lower address. The result is a loss of communication with your subsystem. You must reconfigure and restart your Agent to have it recognize either the new CCL address or the address of an existing virtual disk used for communication.

Interpreting SNMP Traps

B

This chapter describes how to understand an SNMP trap. When a physical storage device, a logical storage unit, or a physical enclosure component changes state, the HS-Series Agent sends an SNMP trap to every system where the SNMP option is enabled. The trap is displayed in the Agent's list of client system entries.

An Agent SNMP trap consists of the following information fields:

■ Source IP address

■ GENERIC = 6 (6 = ENTERPRISE-SPECIFIC VALUE TO FOLLOW)

■ SPECIFIC = 0 or 1, where:

— "0" indicates that the storage component transitioned from a bad to a good state.

— "1" indicates that the storage component transitioned from a good to a bad state.

■ Object ID (OID) variable of the offending storage component

■ OCTET STRING value returning the name of the subsystem containing the storage component specified by the OID Variable

Object ID (OID) Variables

Each OID is prefixed by a Base Enterprise Number (BEN) for the Command Console product. The default BEN for Command Console Agents is as follows:

```
1.3.6.1.4.1.36.2.15.21
(iso.org.dod.internet.private.enterprises.dec.ema.sysobjects.raidmanager)
```

The following are the OID values used by Command Console:

■ Disk Status = BEN + .3.2.1.4

```
(BEN + .subsys.ssStatusTable.ssEntry.ssDiskStatus)
```

■ Power Supply Status = BEN + .3.2.1.5

```
(BEN + .subsys.ssStatusTable.ssEntry.ssPowerStatus)
```

■ Cooling Status = BEN + .3.2.1.6

```
(BEN + .subsys.ssStatusTable.ssEntry.ssFanStatus)
```

■ Cache Battery Charge Status = BEN + .3.2.1.7

```
(BEN + .subsys.ssStatusTable.ssEntry.ssCacheBatteryStatus)
```

■ OverTemperature Status = BEN + .3.2.1.8

```
(BEN + .subsys.ssStatusTable.ssEntry.ssTemperatureStatus)
```

■ Communication Status = BEN + .3.2.1.9

```
(BEN + .subsys.ssStatusTable.ssEntry.ssCommStatus)
```

■ EMU External Input Status = BEN + .3.2.1.10

```
(BEN + .subsys.ssStatusTable.ssEntry.ssEmuExtInputStatus)
```

■ THIS Controller Status = BEN + .3.2.1.12

```
(BEN + .subsys.ssStatusTable.ssEntry.ssController1Status)
```

■ OTHER Controller Status = BEN + .3.2.1.19

```
(BEN + .subsys.ssStatusTable.ssEntry.ssController2Status)
```

■ LUN Status = BEN + .3.2.1.27

```
(BEN + .subsys.ssStatusTable.ssEntry.ssLUNStatus)
```

If your SNMP Management Utility has the Agent MIB compiled, the utility should display the character string values shown in parentheses above. Note that some OID values specified in the MIB are not used for SNMP traps.

Octet String Values

The octet string value attached to a trap takes the form:

```
subsystem_name controller_type ID:state
```

where *subsystem_name* is the name of the subsystem to which the trap applies, *controller_type* is the model number of the controller in the subsystem, *ID* is the identification of the storage component that caused the trap, and *state* is the status of the storage component that caused the trap

Note: A storage component can be a physical storage device, a logical storage unit, or a physical enclosure component.

ID and State Values

The range of values in the ID and status value fields varies, depending upon the type of storage component causing a trap. Acceptable values for various components are as follows:

■ For disk drives:

```
disk_name:state
```

where *disk_name* is the name of the disk drive in the subsystem and *state* is either of the following:

1—Drive went from bad to good.
2—Drive went from good to bad.

■ For temperature sensors:

```
cabinet_number:sensor_type:state
```

where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure, *sensor_type* is the EMU sensor, sensor 1, or sensor 2 in a 2100 enclosure, and state is either of the following:

1—Temperature went from bad to good.
2—Temperature went from good to bad.

■ For cabinet fans:

```
cabinet_number:fan_position:state
```

where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure *fan_position* is the fan location, from 1-3, and
state is either of the following:

1—Went from bad to good.
2—Fan went from good to bad.

■ For power supplies:

```
cabinet_number:pwr_position:state
```

where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure *pwr_position* is the power supply location, from 1-2, and
state is either of the following:

1—Power supply went from bad to good.
2—Power supply went from good to bad.
3—Power supply not present.

■ For batteries:

`controller_device_scsi_id:state`

where *controller_device_scsi_id* is the SCSI ID of the reporting controller on the controller's device bus and *state* is either of the following:

Good—Battery is good.
Low—Battery voltage is low.
Fail—Battery has failed.

■ For LUNs:

virtual_disk_number:state

where *virtual_disk_number* is the unit number of the virtual disk and *state* is either of the following:

0— Good.
1—Reduced.
2—Reconstructing.
3—Failed.

Trap Example

An example SNMP trap for subsystem "subsys1" with a failing power supply on an Agent at IP address "16.82.16.01" would contain the following information:

```
Source address = 16.82.16.01
GENERIC = 6
SPECIFIC = 1
OID Value = 1.3.6.1.4.1.36.2.15.21.3.2.1.5
(iso.org.dod.internet.private.enterprises.
dec.ema.sysobjects.raidmanager.subsys.ssStatusTable.ssEntry.ssP
owerStatus)
OCTET STRING = subsys1 HSZ70 1:3:2

--
-- iso(1) org(3) dod(6) internet(1) private(4) enterprises(1)
dec(36)
-- ema(2) sysobjids(15) raidmanager(21)
RAIDMANAGER-MIB DEFINITIONS::= BEGIN


imports
 enterprises
 FROM RFC1155-SMI
 OBJECT-TYPE
 FROM RFC-1212
 Displaystring
FROM RFC-1213;


dec             OBJECT IDENTIFIER ::= { enterprises 36 }
ema             OBJECT IDENTIFIER ::= { dec 2 }
sysobjids       OBJECT IDENTIFIER ::= { ema 15 }
raidmanager     OBJECT IDENTIFIER ::= { sysobjids 21 }


-- raidmanager MIB
agent           OBJECT IDENTIFIER ::= { raidmanager 1 }
workstation     OBJECT IDENTIFIER ::= { raidmanager 2 }
subsys          OBJECT IDENTIFIER ::= { raidmanager 3 }

--      Agent Information Group

agManufacturer OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
```

```
   "The name of the Enterprise Storage Manager Agent
manufacturer."
  ::= { agent 1 }
agMajVersion OBJECT-TYPE
     SYNTAX   INTEGER
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "Enterprise Storage Manager Agent Major Version Number
(e.g., 3 for 3.0)."\
    ::= { agent 2 }
agMinVersion OBJECT-TYPE
     SYNTAX   INTEGER
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION   "Enterprise Storage Manager Agent Minor
Version Number (e.g., 0 for 3.0)."
    ::= { agent 3 }
agHostName OBJECT-TYPE
     SYNTAX   DisplayString
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "The Host System Network Name where the agent resides."
    ::= { agent 4 }
agEnterprise OBJECT-TYPE
     SYNTAX   OBJECT IDENTIFIER
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "The Enterprise ID subtree for Enterprise Storage Manager
Agent MIB is registered."
::= { agent 5 }
agDescription OBJECT-TYPE
     SYNTAX   DisplayString
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "The Enterprise Array Storage Agent description."
::= { agent 6 }


-- Workstation Group

wsCPU OBJECT-TYPE
     SYNTAX   DisplayString
     ACCESS   read-only
     STATUS   mandatory
```

```
                    DESCRIPTION
               "The workstation CPU type (e.g., 80486)."

               ::= { workstation 1 }
     wsComputerType OBJECT-TYPE
          SYNTAX  DisplayString
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
          "The workstation Computer type (e.g., PC/AT)."

          ::= { workstation 2 }
     wsModel OBJECT-TYPE
          SYNTAX  INTEGER
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
          "The workstation model number."

          ::= { workstation 3 }
     wsSubModel OBJECT-TYPE
          SYNTAX  INTEGER
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
          "The workstation submodel number."

          ::= { workstation 4 }
     wsBiosVersion OBJECT-TYPE
          SYNTAX  DisplayString
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
          "The workstation BIOS Version."

          ::= { workstation 5 }
     wsOS OBJECT-TYPE
          SYNTAX  DisplayString
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
          "The workstation operating system name (e.g., WINNT)."

          ::= { workstation 6 }
     wsOSMajVersion OBJECT-TYPE
          SYNTAX  INTEGER
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
```

```
        "The workstation OS major version number  (e.g., 3 for
WINNT 3.51)."
   ::= { workstation 7 }
wsOSMinVersion OBJECT-TYPE
     SYNTAX   INTEGER
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "The workstation OS minor version number (e.g., 51 for
WINNT 3.51)."
        ::= { workstation 8 }
-- Subsystem Group

ssTotalSubSystems OBJECT-TYPE
     SYNTAX   INTEGER
     ACCESS   read-only
     STATUS   mandatory
     DESCRIPTION
     "The total number of subsystems presently serviced by this
agent."
        ::= { subsys 1 }
-- Subsystem Status Group

ssStatusTable OBJECT-TYPE
     SYNTAX   SEQUENCE OF SsEntry
     ACCESS   not-accessible
     STATUS   mandatory
     DESCRIPTION
     "This table holds the status information for each
subsystem."
        ::= { subsys 2 }
ssEntry OBJECT-TYPE
     SYNTAX   SsEntry
     ACCESS   not-accessible
     STATUS   mandatory
     DESCRIPTION
     "The subsystem information entry."
     INDEX    { ssEntryIndex }

        ::= { ssStatusTable 1 }
SsEntry ::=

   SEQUENCE{
ssEntryIndex
INTEGER,
ssSubsysName
DisplayString,
ssOverallStatus
INTEGER,
ssDiskStatus
INTEGER,
```

```
ssPowerStatus
INTEGER,
ssFanStatus
INTEGER,
ssCacheBatteryStatus
INTEGER,
ssTemperatureStatus
INTEGER,
ssCommStatus
INTEGER,
ssEmuExtInputStatus
INTEGER,
ssEmuPresent
INTEGER,
ssController1Status
INTEGER,
ssController1SerNum
DisplayString,
ssController1RDAC
INTEGER,
ssController1Type
DisplayString,
ssController1ProdID
DisplayString,
ssController1FwRev
DisplayString,
ssController1HwRev
DisplayString,
ssController2Status
INTEGER,
ssController2SerNum
DisplayString,
ssController2RDAC
INTEGER,
ssController2Type
DisplayString,
ssController2ProdID
DisplayString,
ssController2FwRev
DisplayString,
ssController2HwRev
DisplayString,
ssUpsStatus
INTEGER,
ssLunStatus
INTEGER
}

ssEntryIndex OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
```

```
        DESCRIPTION
        "The index into ssStatusTable .

::= { ssEntry 1 }

ssSubsysName OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
        "The local Subsystem Name."

        ::= { ssEntry 2 }

ssOverallStatus OBJECT-TYPE
        SYNTAX  INTEGER  {
            GREEN(0),
            YELLOW(1),
            RED(2)
          }
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
         "This variable reports the overall status of the
subsystem.
         GREEN: Normal Operating Condition
         YELLOW: Warning Condition
         RED: Subsystem Communication Failure; No response to
Agent requests."

        ::= { ssEntry 3 }

ssDiskStatus OBJECT-TYPE
             SYNTAX  INTEGER  {
                         ALL_OK(0),

AT_LEAST_1_FAILURE(1)
                         }
         ACCESS  read-only
         STATUS  mandatory
         DESCRIPTION
         "This variable reports the overall status for the
          physical devices in the subsystem."

        ::= { ssEntry 4 }

ssPowerStatus OBJECT-TYPE
                 SYNTAX  INTEGER  {
                             ALL_OK(0),
                             AT_LEAST_1_FAILURE(1)
                         }
         ACCESS  read-only
         STATUS  mandatory
         DESCRIPTION
```

```
                        "This variable reports the status for the
                         Power Supply system in the subsystem."
             ::= { ssEntry 5 }

ssFanStatus OBJECT-TYPE
             SYNTAX   INTEGER   {
                            ALL_OK(0),
                            AT_LEAST_1_FAILURE(1)
                       }
      ACCESS   read-only
      STATUS   mandatory
     DESCRIPTION
    "This variable reports the status for the
     FAN system in the subsystem."

      ::= { ssEntry 6 }

ssCacheBatteryStatus OBJECT-TYPE
             SYNTAX   INTEGER   {
                            NORMAL_CHARGE(0),
                            LOW_CHARGE(1)
                       }
      ACCESS   read-only
      STATUS   mandatory
      DESCRIPTION
      "This variable reports the status for the
       Cache Battery in the subsystem. This status object is
currently
       non-functional but in place for future use."

          ::= { ssEntry 7 }

ssTemperatureStatus OBJECT-TYPE
       SYNTAX   INTEGER   {
                       NORMAL(0),
                       OVER_TEMP_CONDITION(1)
                   }
      ACCESS   read-only
      STATUS   mandatory
      DESCRIPTION
      "This variable reports the status for the
       Temperature in the subsystem."

          ::= { ssEntry 8 }

ssCommStatus OBJECT-TYPE
       SYNTAX   INTEGER   {
                    NORMAL(0),
                        COMMUNICATION_FAILURE(1)
                   }
     ACCESS   read-only
      STATUS   mandatory
      DESCRIPTION
```

```
                       "This variable reports the status for the
                        communication to the Primary Controller."

                       ::= { ssEntry 9 }
             ssEmuExtInputStatus OBJECT-TYPE
                     SYNTAX  INTEGER  {
                                  ALL_OK(0),
                                  AT_LEAST_1_FAILURE(1)
                              }
                 ACCESS  read-only
                 STATUS  mandatory
                 DESCRIPTION
                 "This variable reports the status for the
                  EMU external input."

                 ::= { ssEntry 10 }
             ssEmuPresent OBJECT-TYPE
                     SYNTAX  INTEGER  {
                                  EMU_NOT_PRESENT(0),
                                  EMU_PRESENT(1)
                              }
                ACCESS  read-only
                STATUS  mandatory
                  DESCRIPTION
                  "This variable reports the availability of the
                   Environment Monitoring Unit for the subsystem."

                 ::= { ssEntry 11 }
             ssController1Status OBJECT-TYPE
                     SYNTAX  INTEGER  {
                                  NORMAL(0),
                                  FAILED(1)
                              }
                 ACCESS  read-only
                 STATUS  mandatory
                 DESCRIPTION
                 "This variable reports the status for the
                  Primary Controller."

                 ::= { ssEntry 12 }
             ssController1SerNum OBJECT-TYPE
                 SYNTAX  DisplayString
                 ACCESS  read-only
                 STATUS  mandatory
                 DESCRIPTION
                "The Primary Controller's Serial Number."

                 ::= { ssEntry 13 }
             ssController1RDAC OBJECT-TYPE
                   SYNTAX  INTEGER  {
                    SINGLE_MODE(0),
                    DUAL_MODE(1)
                              }
                   ACCESS  read-only
```

```
                        STATUS  mandatory
                        DESCRIPTION
                        "The Primary Controller MODE."

                        ::= { ssEntry 14 }
                ssController1Type OBJECT-TYPE
                        SYNTAX  DisplayString
                        ACCESS  read-only
                        STATUS  mandatory
                        DESCRIPTION
                        "The Primary Controller's Type indicator."

                      ::= { ssEntry 15 }
                ssController1ProdID OBJECT-TYPE
                        SYNTAX  DisplayString
                        ACCESS  read-only
                        STATUS  mandatory
                        DESCRIPTION
                        "The Primary Controller's Product ID."

                      ::= { ssEntry 16 }
                ssController1FwRev OBJECT-TYPE
                        SYNTAX  DisplayString
                        ACCESS  read-only
                        STATUS  mandatory
                        DESCRIPTION
                        "The Primary Controller's Firmware Revision."

                      ::= { ssEntry 17 }
                ssController1HwRev OBJECT-TYPE
                        SYNTAX  DisplayString
                        ACCESS  read-only
                        STATUS  mandatory
                        DESCRIPTION
                        "The Primary Controller's Hardware Revision."

                      ::= { ssEntry 18 }
                ssController2Status OBJECT-TYPE
                    SYNTAX   INTEGER   {
                                    NORMAL(0),
                                    FAILED(1)
                                }
                     ACCESS  read-only
                    STATUS  mandatory
                     DESCRIPTION
                     "This variable reports the status for the
                     Secondary Controller."

                      ::= { ssEntry 19 }
                ssController2SerNum OBJECT-TYPE
                        SYNTAX  DisplayString
                        ACCESS  read-only
                        STATUS  mandatory
```

```
        DESCRIPTION
    "The Secondary Controller's Serial Number."

    ::= { ssEntry 20 }
ssController2RDAC OBJECT-TYPE
    SYNTAX   INTEGER   {
            SINGLE_MODE(0),
            DUAL_MODE(1)
        }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller MODE."

    ::= { ssEntry 21 }
ssController2Type OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller's Type indicator."

    ::= { ssEntry 22 }
ssController2ProdID OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller's Product ID."

    ::= { ssEntry 23 }
ssController2FwRev OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller's Firmware Revision."

    ::= { ssEntry 24 }

    ssController2HwRev OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
    "The Secondary Controller's Hardware Revision."

    ::= { ssEntry 25 }
ssUpsStatus OBJECT-TYPE
    SYNTAX   INTEGER   {
            UPS_NOT_PRESENT(0),
```

```
                                  UPS_PRESENT(1)
                        }
    ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
     "Uninterruptable Power Supply status (Currently for future
use)."
      ::= { ssEntry 26 }

ssLunStatus OBJECT-TYPE
    SYNTAX  INTEGER  {
                        UPS_NOT_PRESENT(0),
                        UPS_PRESENT(1)
                    }
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
     "LUN status."

    ::= { ssEntry 27 }

END
```

glossary

This glossary defines terms used in this guide or related to this product.

adapter	A device that converts the protocol and hardware interface of one bus type into that of another without changing the functionality of the bus.
Agent (HS-Series Agent)	Command Console's secure TCP/IP network communication program. Agent runs on your subsystems' host computer. It is available on several operating systems. One or more Client programs can access the HS-Series Agent running on a host system. Using the system's SCSI or Fibre Channel bus, the Agent can communicate with multiple subsystems on the same host system. You can configure the HS-Series Agent with password protection to prevent unauthorized users from accessing your subsystems.
	Collects data from the devices connected to the HS-Series controller and sends them to the Client. Enables the Client to communicate with storage connected to the HSxxx controller.
Allocation Class	A number that uniquely identifies a controller or group of controllers in a cluster. The allocation class provides a way of grouping disk-based virtual disks across controllers and distinguishing identical virtual disk names within the cluster. Legal values are 0-65535. The allocation class attribute applies to both controllers in a dual-redundant configuration.
array controller	A hardware and software device that provides communication between a system and one or more devices in an array.

Asynchronous Event Service (AES)	AES, which runs as a service in the background, collects and passes all traps from the subsystems to the appropriate Navigation trees and individual pagers. AES needs to be running for the Client to receive updates.
available	A state in which a device is operational but not yet in use as a member of a virtual disk.
Bad Block Replacement (BBR)	Substitution of defect-free device blocks for defective ones. The procedure used to locate a replacement block, mark a bad block as replaced, and move data from the bad block to the replacement block. In some controllers this process occurs automatically.
block	Consecutive bytes of data stored on a storage device. In most subsystems, a block is the same size as a physical disk sector.
blower	An airflow device mounted in a device or controller shelf.
cache	A fast temporary storage buffer in a controller or computer.
capacity	The total amount of data that a physical or virtual disk can store.
channel	A SCSI device bus. Narrow SCSI device buses support up to 7 devices, and wide buses support up to 15 devices. Also called a "port."
chunk	HS-series controller term for strip.
chunk size	HS-series controller term for strip size.
Client	The Command Console uses its associate program -- Agent -- for network connections to multiple subsystems. The Client can use either a serial maintenance port or a host SCSI bus connection to connect to a single subsystem. From the Client, you can view multiple storage systems and set up pager notification.
client list	List of Client nodes that are allowed to connect to an Agent over the network. The list is maintained in the *client.ini* file on the host where the Agent is installed. A client list entry includes the TCP/IP address or network name and the allowed access level for the host's subsystems of each Client.
client system	Computer on which the Client software is installed.

cold swap	Device replacement requiring that you power off the controller and cabinet shelves. This method is used if conditions preclude using the warm swap or hot swap method.
Command Console Client	Provides event notification and the Navigation window.
configuration file	A file in which configuration information for a subsystem is stored. The file can be used to automatically configure the subsystem.
container	HS-series controller term for a device group.
controller	A firmware-driven hardware device used for communication between a host and storage devices. A controller translates bus protocols and hardware interfaces and adds functionality to the subsystem. Some controllers provide additional functionality by mapping storage devices to host-addressable, virtual disks with specific performance and availability features that use RAID techniques.
controller shelf	A shelf designed to contain controller and cache memory modules. A controller shelf can contain two controllers in a dual-redundant configuration.
copy speed	For HS-series controllers, the rate at which the controller writes mirrored data in a mirrored virtual disk. There are two speeds:
	■ Normal -- uses relatively few controller resources to perform the copy and has little impact on controller performance.
	■ Fast -- uses more controller resources, which reduces the time it takes to complete the copy, but also reduces overall controller performance.
device	In its physical form, a magnetic or optical disk, tape, or CD-ROM that can be attached to a SCSI bus. A device provides large amounts of addressable storage to a host.
	This term also means a physical device that is part of a controller's configuration. That is, it is known to the controller. After a device is made known to the controller, you can create virtual disks from it.
device driver	A program that processes I/O requests for a particular type of device.

device group	A logical, internal controller structure representing one or more devices that are linked as a group. Some controllers require that you must create device groups before you can create a virtual disk from them. Device groups are also known as containers. There are different types of device groups:

- Single-device virtual disks (JBODs)
- Striped virtual disks (RAID 0)
- Mirrored virtual disks (RAID 1)
- Striped mirrored virtual disks (RAID 0+1)
- Striped parity virtual disks with parity across all drives (RAID 3/5)
- Striped parity virtual disks with floating parity disk (RAID 5)

disk	A storage device that uses rotating magnetic media to store data.
disk array	A collection of disk devices that are physically connected in an ordered structure.
dual-redundant configuration	For HS-series controllers, a configuration consisting of a primary and backup controller in one controller shelf. If the primary controller fails, the backup controller assumes control of the failing controller's devices.
Environmental Monitoring Unit (EMU)	Some subsystem enclosures include an environmental monitoring unit that provides increased protection against catastrophic faults. The EMU works with the controller to warn about impending subsystem failures. The EMU senses such conditions as failed power supplies, failed blowers, elevated temperatures, and external air sense faults.
failed	A device state indicating that a device is inoperable and unavailable for use in a virtual disk. In some controllers, you can force a failed state, for instance to remove the device from the storage enclosure. In others, a device is marked as failed if you remove it as a member of a virtual disk.

failover	For HS-Series controllers, the process that takes place when one controller in a dual-redundant configuration fails and the other controller takes over. The other controller continues to direct the subsystem until the failed controller is again operational or is replaced.
good	A device state that indicates that a device is operational and in use by a virtual disk.
host	The primary or controlling computer to which a subsystem is attached.
host access ID	The target ID of the host computer allows exclusive access to a particular virtual disk. A virtual disk can be set to allow all or only one host target ID access to it.
host adapter	A device connecting a host system to a SCSI bus. Typically, the host adapter performs the functions of the lowest layers of the SCSI protocol. This function may be logically and physically integrated into the host system.
host functionality	You can configure your controller's host port targets for optimum performance and compatibility.
hot disks	Hot disks occur if the workload is poorly distributed across storage devices. A hot disk is a device with multiple hot spots. On a hot disk, host I/O requests begin to back up because of the concentrated request load. Hot disks cause subsystem performance to suffer.
hot spare	In a virtual disk, a device configured to automatically replace a failed device. If a virtual disk member fails, the controller automatically replaces the member with the spare device, and it rebuilds the member's data from the remaining devices in the virtual disk.
hot spots	Hot spots occur if the workload is poorly distributed across storage devices. A hot spot is a file or a group of files located on the same device that receive a very high concentration of I/O requests.
hot swap	A method of device replacement in which the system remains operational during device removal and reinstallation. The device being removed or reinstalled is the only device that is not operational during the process.

HSxxx Client	Provides the HSxxx Storage window for storage connected to the HSxxx controller.
initialization	For subsystems, the process of restarting the controllers and reestablishing the subsystem's configuration and operation; that is, bootstrapping the subsystem. For virtual disks, the process of writing the controller's file structure to the virtual disk member devices. On the member disks, the file structure is represented by metadata.
JBOD (Just a Bunch of Disks)	JBOD is an industry term for a single-device virtual disk. A JBOD virtual disk does not provide any level of data redundancy.
known client list	See client list.
Local Area Network (LAN)	A network that is confined to a single geographic location.
local connection	A direct hardware connection from the Client to a single subsystem using either of two methods:

■ A connection from a standalone computer running the Client to the serial maintenance port on the controller

■ A connection from a host system running the Client to a subsystem on the host's SCSI bus

A local connection enables you to connect the Client to one subsystem controller within the physical range of the serial or host SCSI cable.

logical drive	See virtual disk.
logical storage unit	See virtual disk.
Logical Unit Number (LUN)	A SCSI bus supports a number of target devices, each of which has a number of logical units. A logical unit number is a logical unit's address on a target. A controller maps one or more SCSI logical units to a virtual disk that the host can access. "LUN" is also used to refer to the virtual disk itself.
mapping	The internal controller process of organizing single or grouped devices into virtual storage units (that is, virtual disks).

maximum block transfer	For HS-series controllers, the virtual disk parameter that specifies the maximum number of data blocks to be cached before writing data to virtual disk members. A data transfer greater than this size is not cached and is written immediately to disk. Valid values are 1-1024 (blocks).
member	Any device used in a virtual disk based on multiple devices. Any device in the device group on which the virtual disk is based.
metadata	Special data written to a device for the purpose of controller administration. Metadata improves error detection and media defect management for a device. It is also used to define device and virtual disk configuration.
mirrored cache	Some controllers offer high-performance cache hardware that can be set to operate in mirrored mode. In this mode, the cache data is duplicated and stored in cache memory in physically separate locations. If one copy of the data becomes corrupted or unavailable for some reason, the other copy is available for use.
	A mirrored cache configuration provides complete protection for cached data. However, the cache memory effectively contains twice as much data for each host request, so the effective size of the cache is cut in half.
mirrored virtual disk	A group of storage devices organized as duplicate copies of each other. Mirrored virtual disks provide the highest level of data availability at the highest cost. Another name for RAID 1.
mirroring	The simplest form of data redundancy. Two or more devices form a mirrored device group. Each device is an exact copy of the other.
	For read requests, data can be read from either device therefore increasing the throughput. Both devices can handle different requests simultaneously.
	For write requests, data is written to both devices. If one device fails, all reads/writes are executed on the mirrored device group's other device. Therefore, mirroring provides excellent availability (unless the second device fails before the first (failing) device can be repaired or replaced).
	Sometimes called shadowing.
	The mirroring technique can also be applied to cache memory.

Navigation tree	Provides access to the HSxxx Storage window
	Displays the status of your systems in a hierarchical order.
Navigation window	It contains the Navigation tree and the menu options for configuring pager notification and the Navigation tree.
network connection	A remote connection from the Client to multiple subsystems using Agent over a TCP/IP-compatible network. Network connections enable you to concurrently monitor thousands of subsystems over a LAN or WAN anywhere in the world.
nonredundant	For HS-series controllers, a single-controller configuration.
	The term is also sometimes used to refer to a RAID level that does not provide fault tolerance (for example, RAID 0).
normal	In mirrored virtual disks, a member state that indicates that a member contains exactly the same data as the other members do
parameter	A setting or value that defines a particular operating characteristic of a device, virtual disk, controller, or subsystem.
parity	Binary value calculated from user data used to detect if associated data becomes corrupt. Parity can also be used to correct corrupted data. Striped parity virtual disks use parity to improve data availability.
parity check	A virtual disk state that indicates that the controller is checking the integrity of a virtual disk's data.
partition	A logical division of a virtual disk, represented itself as a virtual disk to the host. Command Console enables the creation of virtual device partitions, but they are transparent to the user.
password	A code string used by the Client with network connections to restrict configuration functions to privileged users. Passwords are set at the Agent at each host.
pedestal	A desk-side, floor-standing, storage enclosure capable of housing one or more controllers and associated devices to make up a complete subsystem.
physical device	A storage component installed in a subsystem.
physical disk	A storage component with rotating magnetic media that is installed in a subsystem.

port	The hardware and software used to connect a host controller to a communications bus, such as a SCSI bus or serial bus. On the device side of the controller, a port is called a channel. The term is sometimes also used to refer to the logical TCP/IP port that is used to access the Agent over the network.
port/target/LUN (PTL)	For HS-series controllers, the complete address of a physical disk on a device bus from which the controller derives the device name. The name, "disk11300", for instance, indicates a physical device at port 1, target 13, and LUN 00.
RAID (Redundant Array of Independent Disks)	RAID is an industry-standard set of techniques for configuring an array of storage devices into host-accessible, virtual disks with various cost, availability, and performance options.

Some common RAID levels are RAID 0, RAID 1, RAID 0+1, RAID 3, RAID 3/5, and RAID 5. |
| **RAID 0** | RAID 0 is the industry-standard name for disk striping. A RAID 0 virtual disk is also called a striped virtual disk.

In a RAID 0 virtual disk, host data is divided into strips spread in a stripe across virtual disk member devices. This technique provides much faster read and write performance than does reading and writing to a single device. A three-device, RAID 0 virtual disk has potentially three times the bandwidth of a single device because three separate small pieces of host data move in parallel.

RAID 0 is the only RAID level that does not provide some level of data redundancy. Because more devices can potentially fail and because there is no way to recover data for a failed device, RAID 0 virtual disks have less availability than equivalent-sized single disks. |

RAID 0+1   RAID 0+1 combines the striping of RAID 0 and the mirroring
                      of RAID 1 to provide the best combination of high performance
                      and high availability. A RAID 0+1 virtual disk is also known as
                      a striped mirrored virtual disk.

                      In a RAID 0+1 virtual disk, each RAID 0 stripe is mirrored to
                      one or more duplicate device sets. This technique allows much
                      faster read and write performance than does reading and writing
                      to a single device. A six-device, RAID 0+1 virtual disk has
                      potentially three times the bandwidth of a single device because
                      three separate, small pieces of host data move in parallel.

                      In addition, the data is completely mirrored to one or more
                      device sets so there is complete data redundancy for very high
                      availability.

                      A RAID 0+1 virtual disk offers the highest performance and the
                      highest availability of any RAID virtual disk type, but its cost is
                      high. Such a configuration requires at least twice the number of
                      devices that a RAID 0 configuration requires.

RAID 1   RAID 1 is the industry-standard term for device mirroring. A
                      RAID 1 virtual disk is also called a mirrored virtual disk.

                      In a RAID 1 virtual disk, host data is written as a single large
                      block to one device and the data is mirrored to one or more
                      duplicate disks.

                      A RAID 1 virtual disk provides very high availability because
                      the data is completely mirrored to one or more devices. Its
                      performance is no better than that of a single device, however,
                      because the data is transferred as one large block to and from
                      these devices.

RAID 3   RAID 3 virtual disks use parity for data redundancy. A RAID 3 virtual disk is a type of striped parity virtual disk.

In a RAID 0 virtual disk, host data is divided into strips spread in a stripe across virtual disk member devices. An additional strip for parity information is appended to each stripe. This technique allows much faster read and write performance than does reading and writing to a single device. A three-device, RAID 3 virtual disk has potentially three times the bandwidth of a single device because three separate, small pieces of host data move in parallel.

In addition, because each data stripe is protected by parity information, there is a significant level of data redundancy for high availability. Some RAID 3 configurations use a dedicated parity device, but most controllers intersperse the parity strips within the data strips to maximize the read performance.

RAID 3 virtual disks provide high performance and high availability at reasonable cost. They are optimal for use in applications requiring relatively high data transfer rates and having relatively low I/O request rates.

RAID 3/5   RAID 3/5 sets are enhanced stripesets – they use striping to increase I/O performance and distributed-parity data to ensure data availability.

RAID 3/5 sets are similar to stripesets in that the I/O requests are broken into smaller "chunks" and striped across the disk drives. RAID sets also create chunks of parity data and stripe them across all members of the RAIDset. This parity data is derived mathematically from the I/O data and enables the controller to reconstruct the I/O data if a single disk drive fails. Thus, it becomes possible to lose a disk drive without losing its data it contained. Data can be lost, however, if a second disk drive fails before the controller replaces the first failed disk drive and reconstructs the data.

RAID 5

RAID 5 virtual disks use parity for data redundancy. A RAID 5 virtual disk is a type of striped parity virtual disk.

In a RAID 5 virtual disk, host data is written in its entirety as a strip representing one I/O request into a much larger stripe of I/O requests stored across the virtual disk membership. An additional strip for parity information is written into each stripe. This technique offers the same read performance as reading from a single device. However, in a RAID 5 virtual disk, multiple read I/O requests can occur resulting in a very high overall subsystem read performance.

Write performance, however, is much worse. Because writing a small strip of data into a larger amount of data on a device is really a read-modify-write operation, writing becomes time-consuming. In addition, because each data stripe is protected by parity information, there is a significant level of data redundancy for high availability.

RAID 5 virtual disks provide high read performance and high availability at reasonable cost. They are optimal for use in applications that have relatively high I/O read request rates and require relatively low data transfer rates.

read cache

A block of high-speed memory used to buffer data being read from storage devices by a host. A read cache responds to host read requests from local cache memory if possible rather than from external storage devices. Therefore, it increases the controller's effective device access speed.

The controller maintains copies of data recently requested by the host in cache, and it may fetch blocks of data ahead of a request in anticipation that the controller will access the next sequential blocks. In a typical read cache, host write requests are handled without involving caching.

read source	For HS-series controllers, a mirrored virtual disk option that controls the way data is read from the virtual disk's members. There are two Read Source options:
	■ Least Busy (default) -- the Normal, virtual disk member with the smallest I/O load is the target of all read operations.
	■ Round Robin -- each Normal, virtual disk member is the target of a read operation in sequential membership order. No preference is given to any member.
rebuild rate	The rate at which the controller reconstructs a failed device on a spare. To devote more or fewer cycles to rebuilding a failed device on a spare, adjust the rate using a scale from 1-100. A rebuild rate of 100 rebuilds the device at the fastest rate possible.
reconstructing	A physical device state that indicates that the controller is regenerating a failed device's data onto a replacement device that is part of a redundant virtual disk.
	All user data remains available during the reconstruction process, but some performance reduction occurs if a request requires access to a device while it is being reconstructed.
reconstruction	Process of regenerating all of a failed member's data, writing it to a spare device, and incorporating the spare device as a redundant RAID virtual disk member.
	All user data remains available during the reconstruction process, but some performance reduction occurs if a request requires access to a device while it is being reconstructed.
reconstruction rate	The speed at which a failed member's data is regenerated. The rate is adjustable. See rebuild rate.
reduced	A virtual disk state that indicates that a member device is missing, failed, or physically removed from a virtual disk.
redundant RAID	Any RAID level that uses redundant information to provide some level of data protection. RAID 1 (mirroring), RAID 0+1 (striped mirroring), RAID 3 (striped parity), RAID 5 (striped parity), and RAID 3/5 (striped parity) virtual disks are all examples of virtual disks that use redundant-RAID techniques.

regeneration	The process of recreating all or a portion of the data from a failed device using the surviving data and parity from the other virtual disk members.
	In most controllers, data from all members remains available during regeneration, and the user is unaware that regeneration is occurring, except for a slight reduction in performance.
	Regeneration of an entire disk member is called reconstruction.
	Data regeneration occurs under one of the following conditions:
	■ The controller detects a hard read error on a virtual disk member. In this case, the controller transparently corrects the data and continues the read operation.
	■ The controller detects that a virtual disk member failed. In this case, the controller completely reconstructs the failed member.
SCSI (Small Computer System Interface)	An industry-standard parallel bus used to interconnect systems and physical devices.
SCSI device	A computer, a host adapter, a peripheral controller, or any storage element that can be attached to a SCSI bus.
SCSI ID	See target ID.
shadowing	See mirroring.
spare	A device state indicting that a device is designated as a hot spare for a failed device within a redundant RAID virtual disk. If a virtual disk member fails, the controller automatically replaces it with a spare device from the pool of spare devices.
	The term is also used to refer to a spare device itself.
storageset	HS-series controller term for device group.
Storage Window	The Storage window is a Client component that provides a graphical interface for configuring and monitoring to a selected subsystem.

strip	A RAID virtual disk using striping stores host data in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips make up a stripe.
	In some controllers, the strip size is used to tune the striped virtual disk for a specific application:
	■ If a virtual disk uses a small strip size compared to the size of the average host request, the controller can break the host data up into strips and can perform device accesses in parallel using RAID 3 techniques. This optimizes the virtual disk for applications requiring high data transfer rates.
	■ If a virtual disk uses a large strip size compared to the size of the average host request, the controller can use RAID 5 techniques to perform multiple read accesses in parallel on any device. This optimizes the virtual disk for applications requiring high I/O request rates.
	Also called a chunk, segment, or stripe element.
stripe	A RAID virtual disk using striping stores host data in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips across the member devices form a stripe.
strip size	The number of blocks of data that make up a strip.
	In some controllers offering multiple-RAID-level virtual disks such as RAID 3/5, the relationship between the strip size and the average host I/O request size determines how the controller accesses the devices in the virtual disk and affects the request and data transfer performance of the subsystem.
striped virtual disk	Another name for a RAID 0 virtual disk.
striped mirrored virtual disk	Another name for a RAID 0+1 virtual disk.
striped parity virtual disk	Another name for a RAID 3, or RAID 3/5 virtual disk.

striping	A RAID technique in which host data is stored in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips across the member devices form a stripe.
subsystem for the HSxxx controller	A controller and an array of physical devices attached to a host.
supported device	A device tested as functionally compatible with a controller in an approved hardware and software configuration.
surviving controller	The controller in a dual-redundant pair of HS-series controllers that assumes service to its companion's devices when the companion controller fails.
target	A SCSI bus device. When one device addresses another device on a SCSI bus, it uses the target device's target ID to uniquely identify it.
target ID	The physical address a bus initiator uses to connect with a bus target. Each bus target is assigned a unique target address. Also used to refer to a SCSI device ID itself.
TCP/IP	An acronym for Transmission Control Protocol/Internet Protocol. This popular Internet network protocol uses IP addressing, where each network node has a unique network address. The Client uses the TCP/IP to communicate with Agent.
transfer rate	Date transfer speed over a SCSI bus. The transfer rate depends on the bus speed and width. Transfer rates are usually expressed in units of megabytes per second. Some controllers allow you to set the maximum transfer rate on either their host or device bus. This feature allows you to limit the rate in special situations, such as those that require long bus cabling.
unit	See virtual disk.
volume	See virtual disk.
volume set	See virtual disk.

virtual disk	A series of physical drives linked together so that the software interprets the drives as being a single device. Logical storage units are called virtual disks and are accessible by the host. Each virtual disk has its own user-configurable parameters.
	Some controllers use RAID techniques to provide virtual disks with various cost, availability, and performance options.
	Also called logical drives, volumes, volume sets, logical storage units, logical units, units, and LUNs.
warm swap	In some controllers, a feature that allows devices to be added, removed, or replaced while the subsystem remains operational, but with all activity on the controller's device buses stopped.
Wide Area Network (WAN)	A network that spans a large geographic area.
write-back cache	A cache configuration that increases the performance of host write requests. If a host requests a write operation, the controller writes the host's data first to the cache memory, completing the request quickly. It performs the slower operation of flushing data to the external storage device at a later time. The host sees the write operation as complete when the data reaches the cache.
	For most controllers using write-back cache, the cache also increases performance with read cache techniques.
write only	A device state that indicates that while a member was being reconstructed an error was found on another member of the virtual disk.
write-through cache	A technique for handling host write requests in read caches. If the host requests a write operation, the controller writes data directly to the external storage device and updates the cache memory to ensure that the memory does not contain obsolete data. This technique increases the chances that future host read requests can be filled from the cache. The host sees the write operation as complete only after the external storage device is updated.
	For some controller fault conditions, write-back cache resorts to write-through cache operation to protect your data.

index

symbols on equipment 13

T

TCP/IP network 25
technical support, HP 16
Telocator Alphanumeric Protocol (TAP) 46
temperature 48, 83
text symbols 12
third-party storage management program 45, 54
Transmission Control Protocol/Internet Protocol (TCP/IP) network 25, 31, 34, 40
traps 55, 111, 114

U

UNIX host 92
user profiles 46

V

VGA resolution 23, 67
virtual device 69
virtual disk 21
 Command Console 106
 creating 72
 deleting 75
 failure 48

icon 76
LUN address 71
maximum capacity 72
member 72, 76, 100
modifying 76
operating system configuration 77
preserving IDs 108
recovering data 100
state 115
status 67, 83
UNIX configuration 78
Windows NT/2000 configuration 77

W

warning
 rack stability 15
 symbols on equipment 13
web sites
 HP storage 16
Wide Area Network (WAN) 26
Windows 2000/Windows NT 4.0
 Asynchronous Event Service (AES) 42
 disabling CCL 107
 exception 25, 57, 93, 105
 system configuration 94
Windows Internet Name Service (WINS) 25